ISOGENIES OF SUPERSINGULAR ELLIPTIC CURVES OVER FINITE FIELDS AND OPERATIONS IN ELLIPTIC COHOMOLOGY

ANDREW BAKER

Abstract. We investigate stable operations in supersingular elliptic cohomology using isogenies of supersingular elliptic curves over finite fields. Our main results provide a framework in which we give a conceptually simple proof of an elliptic cohomology version of the Morava change of rings theorem and also gives models for explicit stable operations in terms of isogenies and morphisms in certain enlarged isogeny categories. We relate our work to that of G. Robert on the Hecke algebra structure of the ring of supersingular modular forms.

Introduction

In previous work we investigated *supersingular* reductions of elliptic cohomology [4], stable operations and cooperations in elliptic cohomology [3, 5, 6, 8] and in [11, 10] gave some applications to the Adams spectral sequence based on elliptic (co)homology. In this paper we investigate stable operations in supersingular elliptic cohomology using isogenies of supersingular elliptic curves over finite fields; this is similar in spirit to our earlier work [6] on isogenies of elliptic curves over the complex numbers although our present account is largely self contained. Indeed, the promised Part II of [6] is essentially subsumed into the present work together with [8, 11, 10]. A major inspiration for this work lies in the paper of Robert [33], which also led to the related work of [9]; we reformulate Robert's results on the Hecke algebra structure of the ring of supersingular modular forms in the language of the present paper.

Throughout, p will be a prime which we will usually assume to be greater than 3, although much of the algebraic theory works as well for the cases $p = 2, 3$ provided appropriate adjustments are made. The precise implications for elliptic cohomology at the primes 2 and 3 are considerably more delicate and related to work of Hopkins and Mahowald on the ring of topological modular forms.

A very general discussion of useful background material from algebraic geometry can be found in [38].

Historical note. A version of this paper originally appeared around 1998, and grew out of a long period of work on elliptic cohomology in the 1980s sense of a Landweber exact cohomology theory based on level 1 modular forms with 6 inverted. As part of this project the author learned a lot about modular forms and their theory and tried to apply this to stable homotopy theory. The theory described here was an attempt at building a picture of the operations in supersingular elliptic cohomology based on work of Tate and others. We did not make use of the modern theory of structured ring spectra, so this lacks the spectrum-level rigidity that is now seen as crucial in the construction of the topological modular forms spectrum. Nevertheless, recent work of Behrens and Lawson [14, 15] has touched on similar ideas but in a more sophisticated

2000 *Mathematics Subject Classification.* primary 55N34, 55N20, 55N22, 55S05; secondary 14H52, 14L05.

Key words and phrases. elliptic cohomology, supersingular elliptic curve, isogeny.

I would like to thank K. Buzzard, I. Connell, J. Cremona, R. Odoni, N. Strickland, G. Robert, J. Tate and V. Gorbounov for their contributions to my understanding of supersingular elliptic curves over finite fields and also the referee of an earlier version.

Glasgow University Mathematics Department preprint no. 98/39 [Version 13: 12/12/2007].

fashion. We make this paper available on `arXiv` in part to provide a historical record of an earlier attempt at using some of these ideas.

1. Elliptic curves over finite fields

General references for this section are [22, 37], while [25, 26] provide more abstract formulations. We will be interested in elliptic curves $\mathcal{E}$ defined over a subfield $\Bbbk \subseteq \overline{\mathbb{F}}_p$, the algebraic closure of $\mathbb{F}_p$, indeed, we will take $\Bbbk = \overline{\mathbb{F}}_p$ unless otherwise specified. We will impose further structure by prescribing a sort of 'orientation' for a curve as part of the data. We will usually assume that $p > 3$, although most of the algebraic details have analogues for the primes 2 and 3.

We adopt the viewpoint of [25, 26], defining an *oriented elliptic curve* to be a connected 1-dimensional abelian group scheme $\mathcal{E}$ over $\Bbbk$ equipped with a nowhere vanishing invariant holomorphic 1-form $\omega \in \Omega^1(\mathcal{E})$. We will refer to $\mathcal{E}$ as the underlying elliptic curve of $\underline{\mathcal{E}} = (\mathcal{E}, \omega)$.

A morphism of abelian varieties $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ for which $\varphi^*\omega_2 \neq 0$ corresponds to a morphism $\varphi\colon \underline{\mathcal{E}_1} \longrightarrow \underline{\mathcal{E}_2}$. Since $\Omega^1(\mathcal{E}_1)$ is 1-dimensional over $\overline{\mathbb{F}}_p$, there is a unique $\lambda_\varphi \in \Bbbk^\times$ for which $\varphi^*\omega_2 = \lambda_\varphi\omega_1$. So such a morphism φ is a pair of the form $(\varphi, \lambda_\varphi)$; if $\lambda_\varphi = 1$ we will say that φ is *strict*. We will denote the category of all such abstract oriented elliptic curves over $\Bbbk$ by $\mathbf{AbsEll}_\Bbbk$, and $\mathbf{AbsEll}$ when $\Bbbk = \overline{\mathbb{F}}_p$.

If $p > 3$, by the theory of normal forms to be found in [22, 37, 39], for the oriented elliptic curve $\underline{\mathcal{E}}$ there are (non-unique) meromorphic functions X, Y with poles of orders 2 and 3 at $\mathrm{O} = [0, 1, 0]$ and a non-vanishing 1-form $\mathrm{d}X/Y$ for which

$$Y^2 = 4X^3 - aX - b \quad \text{for some } a, b \in \Bbbk. \tag{1.1}$$

The projectivization $\mathcal{E}_{\mathrm{W}}$ of the unique non-singular cubic

$$y^2 = 4x^3 - ax - b \tag{1.2}$$

is a non-singular Weierstaraß cubic and there is an isomorphism of elliptic curves

$$(\theta, \lambda_\theta)\colon (\mathcal{E}, \mathrm{d}X/Y) \longrightarrow (\mathcal{E}_{\mathrm{W}}, \mathrm{d}x/y).$$

By twisting, we can ensure that $\lambda_\theta = 1$, *i.e.*, θ is strict. For each $\underline{\mathcal{E}}$ we choose such a strict isomorphism $\theta_{\underline{\mathcal{E}}}$. Conversely, a Weierstraß cubic yields an abstract elliptic curve with the non-vanishing invariant 1-form $\mathrm{d}x/y$. Let $\mathbf{Ell}$ denote the full subcategory of $\mathbf{AbsEll}$ consisting of such Weierstraß cubics $\mathcal{E}$ equipped with their standard 1-forms, $(\mathcal{E}, \mathrm{d}x/y)$.

Theorem 1.1. *The embedding* $\mathbf{Ell} \longrightarrow \mathbf{AbsEll}$ *is an equivalence of categories.*

Because of this, the phrase (oriented) elliptic curve will now refer to a Weierstraß cubic, since we can replace a general elliptic curve by a Weierstraß cubic up to isomorphism.

A modular form f of weight n defined over $\Bbbk$ is a rule which assigns to each oriented elliptic curve $\underline{\mathcal{E}} = (\mathcal{E}, \omega)$ over $\Bbbk$ a section $f(\underline{\mathcal{E}})\omega^{\otimes n}$ of the bundle $\Omega^1(\mathcal{E})^{\otimes n}$, such that for each isomorphism $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$,

$$\varphi^*(f(\underline{\mathcal{E}_2})\omega_2^{\otimes n}) = f(\underline{\mathcal{E}_1})\omega_1^{\otimes n}.$$

In particular, if $\varphi^*\omega_2 = \lambda\omega_1$, then

$$f(\underline{\mathcal{E}_2}) = \lambda^{-n} f(\underline{\mathcal{E}_1}),$$

which is formally equivalent to f being a modular form of weight n in the classical sense of [37].

If we rewrite Equation (1.2) in a form consistent with the notation of [37, III §1],

$$\mathcal{E}\colon y^2 = 4x^3 - \frac{c_4(\underline{\mathcal{E}})}{12}x + \frac{c_6(\underline{\mathcal{E}})}{216}, \tag{1.3}$$

the functions c_4, c_6 are examples of such modular forms of weights 4 and 6 respectively. The non-vanishing discriminant function Δ defined by

$$\Delta(\underline{\mathcal{E}}) = \frac{(c_4(\underline{\mathcal{E}})^3 - c_6(\underline{\mathcal{E}})^2)}{1728},$$

is also a modular form of weight 12. In fact the curve $\mathcal{E}$ is defined over the finite subfield $\mathbb{F}_p(c_4(\underline{\mathcal{E}}), c_6(\underline{\mathcal{E}})) \subseteq \overline{\mathbb{F}}_p$ and hence over any finite subfield containing it. The *j-invariant* of $\mathcal{E}$ is

$$j(\underline{\mathcal{E}}) = \frac{c_4(\underline{\mathcal{E}})^3}{\Delta(\underline{\mathcal{E}})} \in \mathbb{F}_p(c_4(\underline{\mathcal{E}}), c_6(\underline{\mathcal{E}})).$$

j is a modular form of weight 0 and only depends on $\mathcal{E}$, so we will write $j(\mathcal{E})$.

The next result is well known [22, 37]; note that further information is required to determine the isomorphism class over a finite field containing $\mathbb{F}_p(c_4(\underline{\mathcal{E}}), c_6(\underline{\mathcal{E}}))$.

Theorem 1.2. *The invariant $j(\mathcal{E})$ is a complete isomorphism invariant of the curve $\mathcal{E}$ over the algebraically closed field $\overline{\mathbb{F}}_p$.*

Another important invariant is the *Hasse invariant* $\mathrm{Hasse}(\underline{\mathcal{E}})$ which is a homogeneous polynomial of weight $p-1$ in $c_4(\underline{\mathcal{E}}), c_6(\underline{\mathcal{E}})$ which have given weights 4 and 6 respectively. The oriented elliptic curve $\underline{\mathcal{E}} = (\mathcal{E}, \omega)$ is said to be *supersingular* if $\mathrm{Hasse}(\underline{\mathcal{E}}) = 0$; again this notion only depends on $\mathcal{E}$ and not the 1-form ω.

Given $\mathcal{E}$ defined over $\Bbbk \subseteq \overline{\mathbb{F}}_p$, we can consider $\mathcal{E}(\Bbbk')$, the set of points defined over an extension field $\Bbbk' \supseteq \Bbbk$. We usually regard $\mathcal{E}(\overline{\mathbb{F}}_p)$ as 'the' set of points of $\mathcal{E}$; thus whenever $\Bbbk \subseteq \Bbbk' \subseteq \overline{\mathbb{F}}_p$, we have

$$\mathcal{E}(\Bbbk) \subseteq \mathcal{E}(\Bbbk') \subseteq \mathcal{E}(\overline{\mathbb{F}}_p).$$

We will also use the notation

$$\mathcal{E}[n] = \ker [n]_{\mathcal{E}} \colon \mathcal{E}(\overline{\mathbb{F}}_p) \longrightarrow \mathcal{E}(\overline{\mathbb{F}}_p),$$

where $[n]_{\mathcal{E}} \colon \mathcal{E} \longrightarrow \mathcal{E}$ is the multiplication by n morphism. Actually, this notation is potentially misleading when $p \mid n$ and should be restricted to the case $p \nmid n$. In Section 4, we will also discuss the general case.

For the elliptic curve $\underline{\mathcal{E}} = (\mathcal{E}, \omega)$, if meromorphic functions X, Y are chosen as in Equation (1.1), there is a local parameter at O, namely $-2X/Y$, vanishing to order 1 at O. In terms of the corresponding Weierstraß form of Equation (1.3), this is the local parameter at $\mathrm{O} = [0, 1, 0]$ given by $t_{\underline{\mathcal{E}}} = -2x/y$. When referring to the elliptic curve $\underline{\mathcal{E}}$, we will often use the notation

$$(\mathcal{E}, c_4(\underline{\mathcal{E}}), c_6(\underline{\mathcal{E}}), t_{\underline{\mathcal{E}}})$$

to indicate that it has Weierstraß form as in Equation (1.3) and local parameter $t_{\underline{\mathcal{E}}}$. We refer to this data as a Weierstraß realization of the elliptic curve $\underline{\mathcal{E}} = (\mathcal{E}, \omega)$.

The local parameter $t_{\underline{\mathcal{E}}}$ has an associated formal group law $F_{\underline{\mathcal{E}}}$ induced from the group structure map $\mu \colon \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}$ by taking its local expansion

$$\mu^* t_{\underline{\mathcal{E}}} = F_{\underline{\mathcal{E}}}(t'_{\underline{\mathcal{E}}}, t''_{\underline{\mathcal{E}}})$$

where $t'_{\underline{\mathcal{E}}}, t''_{\underline{\mathcal{E}}}$ are the local functions on $\mathcal{E} \times \mathcal{E}$ induced from $t_{\underline{\mathcal{E}}}$ by projection onto the two factors. Thus we have a formal group law $F_{\underline{\mathcal{E}}}(Z', Z'') \in \Bbbk[[Z', Z'']]$ if $\mathcal{E}$ is defined over $\Bbbk$. The coefficients of $F_{\underline{\mathcal{E}}}$ lie in the $\mathbb{F}_p$-algebra generated by the coefficients $c_4(\underline{\mathcal{E}}), c_6(\underline{\mathcal{E}})$ and the coefficient of $Z'^r Z''^s$ is a linear combination of the monomials $c_4(\underline{\mathcal{E}})^i c_6(\underline{\mathcal{E}})^j$ with $4i + 6j + 1 = r + s$ and whose coefficients are independent of $\underline{\mathcal{E}}$); in particular, only odd degree terms in Z', Z'' occur.

Given two elliptic curves $\underline{\mathcal{E}}$ and $\underline{\mathcal{E}}'$ together with an isomorphism $\alpha \colon \mathcal{E} \longrightarrow \mathcal{E}'$ of abelian varieties, there is a new formal group law $F^{\alpha}_{\underline{\mathcal{E}}}$ defined by

$$F^{\alpha}_{\underline{\mathcal{E}}}(t'_{\underline{\mathcal{E}}}, t''_{\underline{\mathcal{E}}}) = \alpha^{-1} F_{\underline{\mathcal{E}'}}(\alpha^* t'_{\underline{\mathcal{E}'}}, \alpha^* t''_{\underline{\mathcal{E}'}}).$$

Lemma 1.3. *Let $\underline{\mathcal{E}} = (\mathcal{E}, \omega)$ be an oriented elliptic curve and $\alpha \colon \mathcal{E} \longrightarrow \mathcal{E}$ an automorphism of abelian varieties, then $F_{\underline{\mathcal{E}}}^{\alpha} = F_{\underline{\mathcal{E}}}$.*

Proof. The possible absolute automorphism groups are known from [22, 37] to be given by the following list:

- $\mathbb{Z}/6$ if $j(\mathcal{E}) \equiv 0 \bmod (p)$;
- $\mathbb{Z}/4$ if $j(\mathcal{E}) \equiv 1728 \bmod (p)$;
- $\mathbb{Z}/2$ otherwise.

In each case, provided that $\mathbb{F}_{p^2} \subseteq \Bbbk$, $\mathrm{Aut}_{\Bbbk} \mathcal{E} = \mathrm{Aut}\, \mathcal{E}$, the absolute automorphism group. The assertion follows by considering these possibilities in turn; for completeness we describe them in detail.

When $j(\mathcal{E}) \equiv 0$, the Weierstraß form is

$$y^2 = x^3 + \frac{c_6(\underline{\mathcal{E}})}{216}$$

and

$$F_{\underline{\mathcal{E}}}(X, Y) = \sum_{i+j \equiv 1 \bmod (6)} a_{i,j} X^i Y^j.$$

An automorphism of order 6 has the effect

$$(x, y) \longmapsto (\zeta_6^2 x, \zeta_6^3 y); \quad t_{\underline{\mathcal{E}}} \longmapsto \zeta_6^{-1} t_{\underline{\mathcal{E}}},$$

where ζ_6 is a chosen primitive 6-th root of unity in $\overline{\mathbb{F}}_p$.

When $j(\mathcal{E}) \equiv 1728$, the Weierstraß form is

$$y^2 = x^3 - \frac{c_4(\underline{\mathcal{E}})}{12} x,$$

hence

$$F_{\underline{\mathcal{E}}}(X, Y) = \sum_{i+j \equiv 1 \bmod (4)} a_{i,j} X^i Y^j.$$

An automorphism of order 4 has the effect

$$(x, y) \longmapsto (\zeta_4^2 x, \zeta_4^3 y); \quad t_{\underline{\mathcal{E}}} \longmapsto \zeta_4^{-1} t_{\underline{\mathcal{E}}},$$

where ζ_4 is a chosen primitive 4th root of unity in $\overline{\mathbb{F}}_p$.

Finally, in the last case, an automorphism of order 2 has the effect

$$(x, y) \longmapsto (x, -y); \quad t_{\underline{\mathcal{E}}} \longmapsto -t_{\underline{\mathcal{E}}}.$$

□

Given a Weierstraß realization $\mathcal{E}$ of $\underline{\mathcal{E}}$, defined over $\Bbbk$, for $u \in \Bbbk$, the curve

$$\mathcal{E}^u \colon y^2 = 4x^3 - \frac{u^2 c_4(\underline{\mathcal{E}})}{12} x + \frac{u^3 c_6(\underline{\mathcal{E}})}{216}$$

is the *u-twist* of $\mathcal{E}$. For $v \in \Bbbk$ with $v^2 = u$, there is a *twisting isomorphism* $\theta_v \colon \mathcal{E} \longrightarrow \mathcal{E}_0$ which is the completion of the affine map

$$\varphi_v \colon (x, y) \longmapsto (v^2 x, v^3 y).$$

The effect of this on 1-forms is given by

$$\theta_v^* \left(\frac{dx}{y} \right) = v^{-1} \omega.$$

Theorem 1.4. *For each oriented elliptic curve $\underline{\mathcal{E}} = (\mathcal{E}, \omega)$ defined over $\Bbbk$, there is a twisting isomorphism $\underline{\mathcal{E}} \longrightarrow \underline{\mathcal{E}_0}$, defined over $\Bbbk$ or a quadratic extension $\Bbbk'$ of $\Bbbk$, where $\underline{\mathcal{E}_0} = (\mathcal{E}_0, dx/y)$ is a Weierstraß elliptic curve of one of the following types:*

- *If $j(\mathcal{E}) \equiv 0 \bmod (p)$,*
$$\mathcal{E}_0 \colon y^2 = 4x^3 - 4;$$
- *if $j(\mathcal{E}) \equiv 1728 \bmod (p)$,*
$$\mathcal{E}_0 \colon y^2 = 4x^3 - 4x;$$
- *if $j(\mathcal{E}) \not\equiv 0, 1728 \bmod (p)$,*
$$\mathcal{E}_0 \colon y^2 = 4x^3 - \frac{27j(\mathcal{E})}{j(\mathcal{E}) - 1728}x - \frac{27j(\mathcal{E})}{j(\mathcal{E}) - 1728}.$$

Proof. The above forms are taken from Husemoller [22]. Given a Weierstraß realization $\mathcal{E}$ of $\underline{\mathcal{E}}$, it is easy to see that $\mathcal{E}$ has the form $\mathcal{E}_0^u$ for some $u \in \Bbbk$, where $\mathcal{E}_0$ has one of the stated forms depending on $j(\mathcal{E})$. Then there is a twisting isomorphism $\theta_v \colon \mathcal{E} \longrightarrow \mathcal{E}_0$ for $v \in \overline{\Bbbk}$ satisfying $v^2 = u$. $\square$

In each of the above cases, the isomorphism $\theta_v \colon \mathcal{E} \cong \mathcal{E}_0$ is defined using suitable choices of twisting parameter u. Although this is ambiguous by elements of the automorphism groups $\operatorname{Aut}\mathcal{E} \cong \operatorname{Aut}\mathcal{E}_0$, we have the following consequence of Lemma 1.3.

Proposition 1.5. *The formal group law $F_{\underline{\mathcal{E}}}$ only depends on $\underline{\mathcal{E}}$, and not on the isomorphism $\mathcal{E} \cong \mathcal{E}_0$, hence is an invariant of $\underline{\mathcal{E}}$.*

When $\mathcal{E}$ is supersingular, we also have the following useful consequence of the well known fact that $j(\mathcal{E}) \in \mathbb{F}_{p^2}$, see [37, Chapter V Theorem 3.1].

Proposition 1.6. *If $\mathcal{E}$ is supersingular, then the coefficients of $F_{\underline{\mathcal{E}_0}}$ lie in the subfield $\mathbb{F}_p(j(\mathcal{E})) \subseteq \mathbb{F}_{p^2}$.*

2. Categories of isogenies over finite fields and their progeny

For elliptic curves $\underline{\mathcal{E}_1}$ and $\underline{\mathcal{E}_2}$ defined over a field $\Bbbk$, an *isogeny* (defined over $\Bbbk$) is a non-trivial morphism of abelian varieties $\varphi \colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$. A *separable isogeny* is an isogeny which is a separable morphism. This is equivalent to the requirement that $\varphi^*\omega_2 \neq 0$, where ω_2 is the non-vanishing invariant 1-form on $\mathcal{E}_2$. An isogeny φ is finite and the *separable degree* of φ is defined by
$$\deg_{\mathrm{s}} \varphi = |\ker \varphi|.$$
If φ is separable then $\deg_{\mathrm{s}} \varphi = \deg \varphi$, the usual notion of degree.

Associated to the oriented elliptic curve $\underline{\mathcal{E}}$ over $\overline{\mathbb{F}}_p$ defined by Equation (1.3), are the p^k-th power curve
$$\mathcal{E}^{(p^k)} \colon y^2 = 4x^3 - \frac{1}{12}c_4(\underline{\mathcal{E}})^{(p^k)}x + \frac{1}{216}c_6(\underline{\mathcal{E}})^{(p^k)}$$
and the $1/p^k$-th power curve
$$\mathcal{E}^{(1/p^k)} \colon y^2 = 4x^3 - \frac{1}{12}c_4(\underline{\mathcal{E}})^{(1/p^k)}x + \frac{1}{216}c_6(\underline{\mathcal{E}})^{(1/p^k)}$$
where for $a \in \overline{\mathbb{F}}_p$, $a^{(1/p^k)} \in \overline{\mathbb{F}}_p$ is the unique element satisfying
$$(a^{(1/p^k)})^{(p^k)} = a.$$
Properties of these curves can be found in [37]. In particular, given an elliptic curve $\underline{\mathcal{E}}$, there is a canonical choice of invariant 1-forms $\omega^{(p^k)}$ and $\omega^{(1/p^k)}$ so that the assignments
$$\underline{\mathcal{E}} = (\mathcal{E}, \omega) \rightsquigarrow (\mathcal{E}^{(p^k)}, \omega^{(p^k)}) = \underline{\mathcal{E}}^{(p^k)},$$
$$\underline{\mathcal{E}} = (\mathcal{E}, \omega) \rightsquigarrow (\mathcal{E}^{(1/p^k)}, \omega^{(1/p^k)}) = \underline{\mathcal{E}}^{(1/p^k)}$$

extend to functors on the category of isogenies; these powering operations on 1-forms can easily be seen in terms of Weierstraß forms where they take the canonical 1-form dx/y on

$$\mathcal{E}\colon y^2 = 4x^3 - \frac{c_4(\underline{\mathcal{E}})}{12}x + \frac{c_6(\underline{\mathcal{E}})}{216}$$

to dX/Y on each of the curves

$$\mathcal{E}^{(p^k)}\colon y^2 = 4x^3 - \frac{1}{12}c_4(\underline{\mathcal{E}})^{(p^k)}x + \frac{1}{216}c_6(\underline{\mathcal{E}})^{(p^k)},$$
$$\mathcal{E}^{(1/p^k)}\colon y^2 = 4x^3 - \frac{1}{12}c_4(\underline{\mathcal{E}})^{(1/p^k)}x + \frac{1}{216}c_6(\underline{\mathcal{E}})^{(1/p^k)}.$$

Proposition 2.1. *Each isogeny $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ has unique factorizations*

$$\varphi = \mathrm{Fr}^k \circ \varphi_s = {}_s\varphi \circ \mathrm{Fr}^k$$

where the morphisms ${}_s\varphi\colon \mathcal{E}_1^{(p^k)} \longrightarrow \mathcal{E}_2$, $\varphi_s\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2^{(p^{1/k})}$ are separable and the morphisms denoted Fr^k are the evident iterated Frobenius morphisms $\mathrm{Fr}^k\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_1^{(p^k)}$, $\mathrm{Fr}^k\colon \mathcal{E}_2^{(p^{1/k})} \longrightarrow \mathcal{E}_2$.

A special case of this is involved in the following.

Proposition 2.2. *For a supersingular curve elliptic curve $\mathcal{E}$ defined over $\Bbbk$, the iterated Frobenius $\mathrm{Fr}^2\colon \mathcal{E} \longrightarrow \mathcal{E}^{(p^2)}$ factors as*

$$\mathrm{Fr}^2\colon \mathcal{E} \xrightarrow{[p]_{\mathcal{E}}} \mathcal{E} \xrightarrow{\lambda} \mathcal{E}^{(p^2)},$$

where λ is an isomorphism defined over $\Bbbk$. In particular, if $\mathcal{E}$ is defined over $\mathbb{F}_{p^2}$ then $\mathcal{E}^{(p^2)} = \mathcal{E}$ and $\lambda \in \operatorname{Aut}\mathcal{E}$.

Now let $\mathcal{E}_1$ and $\mathcal{E}_2$ be defined over $\overline{\mathbb{F}}_p$ and let $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ be a separable isogeny; then there is a finite field $\Bbbk \subseteq \overline{\mathbb{F}}_p$ such that $\mathcal{E}_1$, $\mathcal{E}_2$ and φ are all defined over $\Bbbk$. Later we will make use of this together with properties of zeta functions of elliptic curves over finite fields to determine when two curves over $\overline{\mathbb{F}}_p$ are isogenous.

Associated to an isogeny $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ between two elliptic curves defined over $\Bbbk$ there is a *dual isogeny* $\widehat{\varphi}\colon \mathcal{E}_2 \longrightarrow \mathcal{E}_1$ satisfying the identities

$$\widehat{\varphi} \circ \varphi = [\deg \varphi]_{\mathcal{E}_1}, \quad \varphi \circ \widehat{\varphi} = [\deg \varphi]_{\mathcal{E}_2},$$

where $[n]_{\mathcal{E}}$ denotes the multiplication by n morphism on the elliptic curve $\mathcal{E}$. Localizing the category of separable isogenies of elliptic curves over finite fields by forcing every isogeny $[n]_{\mathcal{E}}$ to be invertible results in a groupoid since every other regular isogeny also becomes invertible. Using the theory of p-primary Tate modules, we will modify this construction to define a larger category which also captures significant p-primary information.

Let $\underline{\mathcal{E}}$ be an elliptic curve over $\overline{\mathbb{F}}_p$ with a Weierstraß form as in Equation (1.3) with its associated local coordinate function $t_{\underline{\mathcal{E}}} = -2x/y$ and its formal group law $F_{\underline{\mathcal{E}}}(X, Y)$. We say that an isogeny $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ is *strict* if

$$\varphi^* t_{\underline{\mathcal{E}_2}} \equiv t_{\underline{\mathcal{E}_1}} \bmod (t_{\underline{\mathcal{E}_1}}{}^2).$$

This condition is equivalent to the requirement that $\varphi^*\omega_2 = \omega_1$, hence a strict isogeny is separable.

For a separable isogeny $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ there is a unique factorization of the form

$$\varphi\colon \mathcal{E}_1 \xrightarrow{\rho} \mathcal{E}_1/\ker\varphi \xrightarrow{\varphi'} \mathcal{E}_2 \tag{2.1}$$

where φ' is an isomorphism, and ρ is a strict isogeny. The quotient elliptic curve $\mathcal{E}_1/\ker\varphi$ is characterized by this property and is constructed explicitly by Vélu [41], who also determines $\rho^* t_{(\mathcal{E}_1/\ker\varphi, \omega)}$, where ω is the 1-form induced by the quotient map.

We will denote by **Isog** the category of elliptic curves over $\overline{\mathbb{F}}_p$ with isogenies $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ as its morphisms. **Isog** has the subcategory **SepIsog** whose morphisms are the separable isogenies. These categories have full subcategories $\mathbf{Isog}_{\mathrm{ss}}$ and $\mathbf{SepIsog}_{\mathrm{ss}}$ whose objects are the supersingular curves.

These categories can be localized to produce groupoids. This can be carried out using dual isogenies and twisting. For the Weierstraß cubic $\mathcal{E}$ defined by Equation (1.3), and a natural number n prime to p, the factorization of $[n]_{\mathcal{E}}$ given by Equation (2.1) has the form

$$[n]_{\mathcal{E}}\colon \mathcal{E} \longrightarrow \mathcal{E}^{n^2} \xrightarrow{\widetilde{[n]}} \mathcal{E}$$

where

$$\mathcal{E}^{n^2}\colon y^2 = 4x^3 - n^4\frac{c_4(\mathcal{E})}{12}x + n^6\frac{c_6(\mathcal{E})}{216}$$

is the twist of $\mathcal{E}$ by $n^2 \in \overline{\mathbb{F}}_p^{\times}$ and $\widetilde{[n]}$ is the map given by

$$[x, y, 1] \longmapsto [x/n^2, y/n^3, 1].$$

If we invert all such isogenies $[n]_{\mathcal{E}}$, then as an isogeny $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ is a morphism of abelian varieties,

$$\varphi \circ [n]_{\mathcal{E}_1} = [n]_{\mathcal{E}_2} \circ \varphi,$$

hence φ inherits an inverse

$$\varphi^{-1} = [n]_{\mathcal{E}_1}^{-1} \circ \widehat{\varphi} = \widehat{\varphi} \circ [n]_{\mathcal{E}_2}^{-1}.$$

The resulting localized category of isogenies will be denoted $\mathbf{Isog}^{\times}$ and the evident localized supersingular category $\mathbf{Isog}_{\mathrm{ss}}^{\times}$. We can also consider the subcategories of separable morphisms, and localize these by inverting the separable isogenies $[n]_{\mathcal{E}}$, *i.e.*, those for which $p \nmid n$. The resulting categories $\mathbf{SepIsog}^{\times}$ and $\mathbf{SepIsog}_{\mathrm{ss}}^{\times}$ are all full subcategories of $\mathbf{Isog}^{\times}$ and $\mathbf{Isog}_{\mathrm{ss}}^{\times}$.

Given $\underline{\mathcal{E}_1} = (\mathcal{E}_1, \omega_1)$, $\underline{\mathcal{E}_2} = (\mathcal{E}_2, \omega_2)$, we extend the action of a separable isogeny $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ to the morphism

$$\underline{\varphi} = (\varphi, \varphi^{*-1})\colon \underline{\mathcal{E}_1} \longrightarrow \underline{\mathcal{E}_2}.$$

So if $\varphi^*\omega_2 = \lambda\omega$,

$$\underline{\varphi}(\mathbf{x}, \omega_1) = (\varphi(\mathbf{x}), \lambda^{-1}\omega_2).$$

We will often just write φ for $\underline{\varphi}$ when no ambiguity is likely to result. Using this construction, we define modified versions of the above isogeny categories as follows. **SepIsog** is the category whose objects are the oriented elliptic curves over $\overline{\mathbb{F}}_p$ and with morphisms

$$(\varphi, \lambda^{-1}\varphi^{*-1})\colon (\mathcal{E}_1, \omega_1) \longrightarrow (\mathcal{E}_2, \omega_2),$$

where $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ is a separable isogeny and $\lambda \in \overline{\mathbb{F}}_p^{\times}$. Thus **SepIsog** is generated by morphisms of the form $\underline{\varphi}$ together with the 'twisting' morphisms $\underline{\lambda}\colon (\mathcal{E}, \omega) \longrightarrow (\mathcal{E}, \omega)$ given by $\underline{\lambda} = (\mathrm{Id}_{\mathcal{E}}, \lambda^{-1})$ which commute with all other morphisms. We can localize this category to form $\mathbf{SepIsog}^{\times}$ with morphisms obtained in an obvious fashion from those of $\mathbf{SepIsog}^{\times}$ together with the $\underline{\lambda}$. There are also evident full subcategories $\mathbf{SepIsog}_{\mathrm{ss}}$ and $\mathbf{SepIsog}_{\mathrm{ss}}^{\times}$ whose objects involve only supersingular elliptic curves.

We end this section with a discussion of two further pieces of structure possessed by our isogeny categories, both being actions by automorphisms of these categories. First observe there is an action of the group of units $\overline{\mathbb{F}}_p^{\times}$ (or more accurately, the multiplicative group scheme $\mathbb{G}_{\mathrm{m}}$) on **Isog** and its subcategories described above, given by

$$\lambda \cdot (\mathcal{E}, \omega) = (\mathcal{E}^{\lambda^2}, \lambda\omega), \quad \lambda \cdot \varphi = \varphi^{\lambda^2},$$

where $\lambda \in \overline{\mathbb{F}}_p^{\times}$, $\varphi\colon (\mathcal{E}_1, \omega_1) \longrightarrow (\mathcal{E}_2, \omega_2)$ is an isogeny and φ^{λ^2} is the evident composite

$$\varphi^{\lambda^2}\colon (\mathcal{E}_1^{\lambda^{-2}}, \lambda^{-1}\omega_1) \longrightarrow (\mathcal{E}_1, \omega_1) \xrightarrow{\varphi} (\mathcal{E}_2, \omega_2) \longrightarrow (\mathcal{E}_2^{\lambda^2}, \lambda\omega_2).$$

The second action is induced by the Frobenius morphisms Fr^k and their inverses. Namely,

$$\mathrm{Fr}^k(\mathcal{E},\omega) = (\mathcal{E}^{(p^k)},\omega^{(p^k)}), \quad \mathrm{Fr}^k\varphi = \varphi^{(p^k)},$$

where for an isogeny $\varphi\colon (\mathcal{E}_1,\omega_1) \longrightarrow (\mathcal{E}_2,\omega_2)$, $\varphi^{(p^k)}$ is the composite

$$\varphi^{(p^k)}\colon (\mathcal{E}_1^{(1/p^k)},\omega_1^{(1/p^k)}) \xrightarrow{\mathrm{Fr}^{-k}} (\mathcal{E}_1,\omega_1) \xrightarrow{\varphi} (\mathcal{E}_2,\omega_2) \xrightarrow{\mathrm{Fr}^k} (\mathcal{E}_2^{(p^k)},\omega_2^{(p^k)}).$$

If $\varphi(x,y) = (\varphi_1(x,y),\varphi_2(x,y))$, then

$$\varphi^{(p^k)}(x,y) = (\varphi_1(x^{1/p^k},y^{1/p^k})^{p^k},\varphi_2(x^{1/p^k},y^{1/p^k})^{p^k}).$$

Similar considerations apply to the inverse Frobenius morphism Fr^{-k}.

3. Recollections on elliptic cohomology

A general reference on elliptic cohomology is provided by the foundational paper of Landweber, Ravenel & Stong [29], while aspects of the level 1 theory which we use can be found in Landweber [28] as well as our earlier papers [5, 4, 6].

Let $p > 3$ be a prime. We will denote by $E\ell\ell_*$ the graded ring of modular forms for $\mathrm{SL}_2(\mathbb{Z})$, meromorphic at infinity and with q-expansion coefficients lying in the ring of p-local integers $\mathbb{Z}_{(p)}$. Here $E\ell\ell_{2n}$ consists of the modular forms of weight n. We have

Theorem 3.1. *As a graded ring,*

$$E\ell\ell_* = \mathbb{Z}_{(p)}[Q,R,\Delta^{-1}],$$

where $Q \in E\ell\ell_8$, $R \in E\ell\ell_{12}$ and $\Delta = (Q^3 - R^2)/1728 \in E\ell\ell_{24}$ have the q-expansions

$$\begin{aligned}
Q(q) =& E_4 = 1 + 240\sum_{1\leqslant r}\sigma_3(r)q^r,\\
R(q) =& E_6 = 1 - 504\sum_{1\leqslant r}\sigma_5(r)q^r,\\
\Delta(q) =& q\prod_{n\geqslant 1}(1-q^n)^{24}.
\end{aligned}$$

The element $A = E_{p-1} \in E\ell\ell_{2(p-1)}$ is particularly important for our present work. Using the standard notation B_n for the n-th Bernoulli number we have

$$A(q) = 1 - \frac{2(p-1)}{B_{p-1}}\sum_{1\leqslant r}\sigma_{p-2}(r)q^r \equiv 1 \bmod (p).$$

We also have $B = E_{p+1} \in E\ell\ell_{2(p+1)}$ with q-expansion

$$B(q) = 1 - \frac{2(p+1)}{B_{p+1}}\sum_{1\leqslant r}\sigma_p(r)q^r.$$

Finally, we recall that there is a canonical formal group law $F_{E\ell\ell}(X,Y)$ defined over $E\ell\ell_*$ whose p-series satisfies

$$\begin{aligned}
[p]_{F_{E\ell\ell}}(X) &= pX + \cdots + u_1X^p + \cdots + u_2X^{p^2} + (\text{higher order terms})\\
&\equiv u_1X^p + \cdots + u_2X^{p^2} + (\text{higher order terms}) && \bmod (p)\\
&\equiv u_2X^{p^2} + (\text{higher order terms}) && \bmod (p,u_1). \qquad (3.1)
\end{aligned}$$

Combining results of [28, 9], we obtain the following in which $\left(\dfrac{-1}{p}\right)$ is the Legendre symbol.

Theorem 3.2. *The sequence p, A, B is regular in the ring $E\ell\ell_*$, in which the following congruences are satisfied:*

$$\begin{aligned} u_1 &\equiv A && \bmod (p);\\ u_2 &\equiv \left(\frac{-1}{p}\right)\Delta^{(p^2-1)/12} \equiv -B^{(p-1)} && \bmod (p, A). \end{aligned}$$

With the aid of this Theorem together with Landweber's Exact Functor Theorem, in both its original form [27] and its generalization due to Yagita [45], we can define *elliptic cohomology* and its *supersingular reduction* by

$$\begin{aligned} E\ell\ell^*(\ ) &= E\ell\ell^* \underset{BP^*}{\otimes} BP^*(\ )\\ {}^{\mathrm{ss}}E\ell\ell^*(\ ) &= (E\ell\ell/(p, A))^*(\ ) \cong E\ell\ell^*/(p, A) \underset{P(2)^*}{\otimes} P(2)^*(\ ), \end{aligned}$$

where as usual, for any graded group M_* we set $M^n = M_{-n}$. The structure of the coefficient ring ${}^{\mathrm{ss}}E\ell\ell_*$ was described in [4] and depends on the factorization of $A \bmod (p)$. In fact, ${}^{\mathrm{ss}}E\ell\ell_*$ is a product of 'graded fields' and the forms of the simple factors of $A \bmod (p)$ are related to the possible j-invariants of supersingular elliptic curves over $\overline{\mathbb{F}}_p$.

Using the definition of supersingular elliptic curves as pairs $(\mathcal{E}, \omega)$, an element $f \in {}^{\mathrm{ss}}E\ell\ell_{2n}$ can be viewed as a family of sections of bundles $\Omega^1(\mathcal{E})^{\otimes n}$ assigning to $(\mathcal{E}, \omega)$ the section $f(\mathcal{E}, \omega)\omega^{\otimes n}$. An isomorphism $\varphi\colon \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ for which $\varphi^*\omega_2 = \lambda\omega_1$ also satisfies

$$\varphi^* f(\mathcal{E}_2, \omega_2)\omega_2^{\otimes n} = f(\mathcal{E}_1, \omega_1)\omega_1^{\otimes n}$$

and so

$$\varphi^* f(\mathcal{E}_2, \omega_2) = \lambda^{-n} f(\mathcal{E}_1, \omega_1).$$

This is formally equivalent to f being a modular form of weight n in the traditional sense.

The ring $E\ell\ell_*/(p)$ is universal for Weierstraß elliptic curves defined over $\overline{\mathbb{F}}_p$ while ${}^{\mathrm{ss}}E\ell\ell_*$ is universal for those which are supersingular, in the sense of the following result.

Proposition 3.3. *The projectivization $\mathcal{E}$ of the cubic*

$$y^2 = 4x^3 - ax - b$$

defined over $\overline{\mathbb{F}}_p$ is an elliptic curve if and only if there is a ring homomorphisms $\theta\colon E\ell\ell_*/(p) \longrightarrow \overline{\mathbb{F}}_p$ for which

$$\theta(Q) = 12a, \quad \theta(R) = -216b.$$

For such an elliptic curve, $\mathcal{E}$ is supersingular if and only if $\theta(A) = 0$.

The first part amounts to the well known fact that the discriminant of $\mathcal{E}$ is $\Delta(\mathcal{E}) = a^3 - 27b^2$, whose non-vanishing is equivalent to the nonsingularity of $\mathcal{E}$. The second part of this result is equivalent to the statement that $\theta(A) = \mathrm{Hasse}(\underline{\mathcal{E}})$, a result which can be found in [22, 37] together with further equivalent conditions.

Next we discuss some cooperation algebras. In [6], we gave a description of the cooperation algebra $\Gamma^0_* = E\ell\ell_*E\ell\ell$ as a ring of functions on the category of isogenies of elliptic curves defined over $\mathbb{C}$. We will be interested in the supersingular cooperation algebra

$${}^{\mathrm{ss}}\Gamma^0_* = {}^{\mathrm{ss}}E\ell\ell_*E\ell\ell = {}^{\mathrm{ss}}E\ell\ell_* \underset{E\ell\ell_*}{\otimes} E\ell\ell_*E\ell\ell \cong {}^{\mathrm{ss}}E\ell\ell_*(E\ell\ell).$$

The ideal $(p, A) \triangleleft E\ell\ell_*$ is invariant under the Γ^0_*-coaction on $E\ell\ell_*$ and hence ${}^{\mathrm{ss}}\Gamma^0_*$ can be viewed as the quotient of Γ^0_* by the ideal generated by the image of (p, A) in Γ^0_* under either the left or equivalently the right unit map $E\ell\ell_* \longrightarrow \Gamma^0_*$. The pair $({}^{\mathrm{ss}}E\ell\ell_*, {}^{\mathrm{ss}}\Gamma^0_*)$ therefore inherits the structure of a Hopf algebroid over $\mathbb{F}_p$.

The Hopf algebroid structure on $({}^{\mathrm{ss}}E\ell\ell_*, {}^{\mathrm{ss}}\Gamma^0_*)$ implies that

$$\mathrm{Spec}_{\mathbb{F}_p}\, {}^{\mathrm{ss}}\Gamma^0_* = \mathbf{Alg}_{\mathbb{F}}({}^{\mathrm{ss}}\Gamma^0_*, \overline{\mathbb{F}}_p)$$

is a groupoid, or at least this is so if the grading is ignored. By the discussion of Devinatz [18, section 1] (see also our Section 7), the grading is equivalent to an action of $\mathbb{G}_{\mathrm{m}}$ which here is derived from the twisting action discussed in Section 1. Let ${}^{\mathrm{ss}}\mathbf{SEllFGL}$ denote the category of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ with the morphism set

$${}^{\mathrm{ss}}\mathbf{SEllFGL}(\underline{\mathcal{E}_1}, \underline{\mathcal{E}_2}) = \{f \colon F_{\underline{\mathcal{E}_1}} \longrightarrow F_{\underline{\mathcal{E}_2}} : f \text{ is a strict isomorphism}\}.$$

There is an action of $\mathbb{G}_{\mathrm{m}}$ on this extending the twisting action on curves, and also an action of the Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. These actions are compatible with the composition and inversion maps. ${}^{\mathrm{ss}}\mathbf{SEllFGL}$ is also a 'formal scheme' in the sense used by Devinatz [18], thus it can be viewed as a pro-scheme and we can consider continuous functions ${}^{\mathrm{ss}}\mathbf{SEllFGL} \longrightarrow \overline{\mathbb{F}}_p$ where the codomain has the discrete topology.

Theorem 3.4. *There is a natural isomorphism of groupoids with $\mathbb{G}_{\mathrm{m}}$-action,*

$$\mathrm{Spec}_{\overline{\mathbb{F}}_p}\, \overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma^0_* \cong {}^{\mathrm{ss}}\mathbf{SEllFGL}.$$

Moreover, $\overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma^0_{2n}$ can be identified with the set of all continuous functions ${}^{\mathrm{ss}}\mathbf{SEllFGL} \longrightarrow \overline{\mathbb{F}}_p$ of weight n and ${}^{\mathrm{ss}}\Gamma^0_{2n} \subseteq \overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma^0_{2n}$ can be identified with the subset of Galois invariant functions.

The proof is straightforward, given the existence of identification of $E\ell\ell_* E\ell\ell$ as

$$E\ell\ell_* E\ell\ell = E\ell\ell_* \underset{MU_*}{\otimes} MU_*MU \underset{MU_*}{\otimes} E\ell\ell_*,$$

and the universality of MU_*MU for strict isomorphisms of formal group laws due to Quillen [1, 32]. We will require a modified version of his result.

Recall from [1, 32] that

$$MU_*MU = MU_*[b_k : k \geqslant 1]$$

with the convention that $b_0 = 1$, and that the coaction is determined by the formula

$$\sum_{k\geqslant 0} \psi b_k T^{k+1} = \sum_{r\geqslant 0} 1 \otimes b_r (\sum_{s\geqslant 0} b_s \otimes 1\, T^{s+1})^{r+1}.$$

This coaction corresponds to composition of power series with leading term T. We can also form the algebras $MU_*[u, u^{-1}]$ and $MU_*[u, u^{-1}][b_0, b_0^{-1}, b_k : k \geqslant 1]$ in which $|u| = |b_0| = 0$ and there is a coaction corresponding to composition of power series with invertible leading term,

$$\sum_{k\geqslant 0} \psi b_k T^{k+1} = \sum_{r\geqslant 0} 1 \otimes b_r (\sum_{s\geqslant 0} b_s \otimes 1\, T^{s+1})^{r+1}.$$

This also defines a Hopf algebroid $(MU_*[u, u^{-1}], MU_*[u, u^{-1}][b_0, b_0^{-1}, b_k : k \geqslant 1])$ whose right unit is given by

$$\eta_R(xu^n) = \eta_R(x) u^{d+n} b_0^n,$$

where $x \in MU_{2d}$ and $\eta_R(x)$ is the image of x under the usual right unit $MU_* \longrightarrow MU_*MU$. There is a ring epimorphism $MU_*[u, u^{-1}][b_0, b_0^{-1}, b_k : k \geqslant 1] \longrightarrow MU_*MU$ under which $u, b_0 \longmapsto 1$ and which induces a morphism of Hopf algebroids

$$(MU_*[u, u^{-1}], MU_*[b_0, b_0^{-1}, b_k : k \geqslant 1]) \longrightarrow (MU_*, MU_*MU).$$

We can form a Hopf algebroid $(E\ell\ell_*[u, u^{-1}], \Gamma_*)$ by setting

$$\Gamma_* = E\ell\ell_*[u, u^{-1}] \underset{MU_*[u,u^{-1}]}{\otimes} MU_*[u, u^{-1}][b_0, b_0^{-1}, b_k : k \geqslant 1] \underset{MU_*[u,u^{-1}]}{\otimes} E\ell\ell_*[u, u^{-1}]$$

and there is an induced morphism of Hopf algebroids

$$(E\ell\ell_*[u,u^{-1}],\Gamma_*) \longrightarrow (E\ell\ell_*,\Gamma^0_*).$$

Similarly, we can define Hopf algebroid $({}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}],{}^{\mathrm{ss}}\Gamma_*)$ with

$${}^{\mathrm{ss}}\Gamma_* = {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}] \underset{MU_*[u,u^{-1}]}{\otimes} MU_*[b_0,b_0^{-1},b_k : k \geqslant 1] \underset{MU_*[u,u^{-1}]}{\otimes} {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}].$$

Now let ${}^{\mathrm{ss}}\mathbf{EllFGL}$ denote the category whose objects are the supersingular oriented elliptic curves over $\overline{\mathbb{F}}_p$ with morphisms being the isomorphisms of their formal group laws; this category is a topological groupoid with $\mathbb{G}_{\mathrm{m}}$-action, containing ${}^{\mathrm{ss}}\mathbf{SEllFGL}$. Using the canonical Weierstraß realizations of Theorem 1.4, we have the following result.

Theorem 3.5. *There is a natural isomorphism of groupoids with $\mathbb{G}_{\mathrm{m}}$-action,*

$$\operatorname{Spec}_{\overline{\mathbb{F}}_p} \overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma_* \cong {}^{\mathrm{ss}}\mathbf{EllFGL}.$$

Moreover, $\overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma_{2n}$ can be identified with the set of all continuous functions ${}^{\mathrm{ss}}\mathbf{EllFGL} \longrightarrow \overline{\mathbb{F}}_p$ of weight n and ${}^{\mathrm{ss}}\Gamma_{2n} \subseteq \overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma_{2n}$ can be identified with the subset of Galois invariant functions.

Later we will give a different interpretation of ${}^{\mathrm{ss}}\Gamma^0_*$ in terms of the supersingular category of isogenies.

4. Tate modules

In this section we discuss Tate modules of elliptic curves over finite fields. While the definition and properties of the Tate module $\mathcal{T}_\ell\mathcal{E}$ for primes $\ell \neq p$ can be found for example in [22, 37], we require the details for $\ell = p$. Suitable references are provided by [42, 43, 19, 20]. Actually, it is surprisingly difficult to locate full details of this material for abelian varieties in the literature, which seems to have originally appeared in unpublished papers of Tate *et al.*

In this section $\Bbbk$ will be a perfect field of characteristic $p > 0$ and $\mathbb{W}(\Bbbk)$ its ring of *Witt vectors*, endowed with its usual structure of a local ring (if $\Bbbk$ is finite it is actually a complete discrete valuation ring). The absolute Frobenius automorphism $x \longmapsto x^p$ on $\Bbbk$ lifts uniquely to an automorphism $\sigma\colon \mathbb{W}(\Bbbk) \longrightarrow \mathbb{W}(\Bbbk)$ and we will often use the notation $x^{(p)} = \sigma(x)$ for this. Let $\mathbb{D}_\Bbbk$ be the *Dieudonné algebra*

$$\mathbb{D}_\Bbbk = \mathbb{W}(\Bbbk)\langle \mathrm{F},\mathrm{V}\rangle,$$

i.e., the non-commutative $\mathbb{W}(\Bbbk)$-algebra generated by the elements F and V subject to the relations

$$\mathrm{FV} = \mathrm{VF} = p, \quad \mathrm{F}a = a^{(p)}\mathrm{F}, \quad a\mathrm{V} = \mathrm{V}a^{(p)},$$

for $a \in \mathbb{W}(\Bbbk)$. Let $\mathbf{Mod}^{\mathrm{f.l.}}_{\mathbb{D}_\Bbbk}$ be the category of finite length $\mathbb{D}_\Bbbk$-modules and $\mathbf{CommGpSch}_\Bbbk[p]$ be the category of finite commutative group schemes over $\Bbbk$ with rank of the form p^d.

Theorem 4.1. *There is an anti-equivalence of categories*

$$\begin{aligned} \mathbf{CommGpSch}_\Bbbk[p] &\longleftrightarrow \mathbf{Mod}^{\mathrm{f.l.}}_{\mathbb{D}_\Bbbk} \\ G &\leftrightsquigarrow \mathrm{M}(G). \end{aligned}$$

Moreover, if $\operatorname{rank} G = p^s$, then $\mathrm{M}(G)$ has length s as a $\mathbb{W}(\Bbbk)$-module.

This result can be extended to $\mathbf{DivGp}_\Bbbk$, the category of *p-divisible groups* over $\Bbbk$.

Theorem 4.2. *There is an anti-equivalence of categories*

$$\begin{aligned} \mathbf{DivGp}_\Bbbk &\longleftrightarrow \mathbf{Mod}^{\mathrm{f.l.}}_{\mathbb{D}_\Bbbk} \\ G &\leftrightsquigarrow \mathrm{M}(G). \end{aligned}$$

Moreover, if $\operatorname{rank} G = p^s$, $\mathrm{M}(G)$ is a free $\mathbb{W}(\Bbbk)$-module of rank s.

A p-divisible group G of rank p^s is a collection of finite group schemes G_n $(n \geqslant 0)$ with $\operatorname{rank} G_n = p^{ns}$ and exact sequences of abelian group schemes

$$0 \longrightarrow G_n \xrightarrow{j_n} G_{n+1} \longrightarrow G_1 \longrightarrow 0$$

for $n \geqslant 0$. The extension of the result to such groups is accomplished by setting

$$\mathrm{M}(G) = \varprojlim_n \mathrm{M}(G_n)$$

where the limit is taken over the inverse system of maps $\mathrm{M}(j_n)\colon \mathrm{M}(G_{n+1}) \longrightarrow \mathrm{M}(G_n)$. The main types of examples we will be concerned with here are the following.

If F is a 1-dimensional formal group law over $\Bbbk$ of height h, then the p^n-series of F has the form

$$[p^n]_F(X) \equiv uX^{p^{nh}} \bmod (X^{p^{nh}+1}) \tag{4.1}$$

where $u \in \Bbbk^\times$. We have an associated p-divisible group $\ker[p^\infty]_F$ of rank p^h with

$$(\ker[p^\infty]_F)_n = \ker[p^n]_F = \operatorname{Spec}(\Bbbk[[X]]/([p^n]_F(X))).$$

Let $\mathcal{E}$ be a supersingular elliptic curve defined over $\Bbbk$. The family of finite group schemes

$$\mathcal{E}[p^n] = \ker[p^n]_{\mathcal{E}} \quad (n \geqslant 0)$$

constitute a p-divisible group $\mathcal{E}[p^\infty]$ of rank p^2. In particular, if $F_{\mathcal{E}}$ is the formal group law associated to the local parameter $t_{\mathcal{E}}$ associated with a Weierstraß equation for $\mathcal{E}$, we have

Lemma 4.3. *If $\mathcal{E}$ is a supersingular elliptic curve defined over $\Bbbk$, there is a compatible family of isomorphisms of group schemes over $\Bbbk$,*

$$\mathcal{E}[p^n] \cong \ker[p^n]_{F_{\mathcal{E}}} \quad (n \geqslant 0),$$

and hence there is an isomorphism of divisible groups

$$\mathcal{E}[p^\infty] \cong \ker[p^\infty]_{F_{\mathcal{E}}}.$$

Proof. This is essentially proved in Silverman [37, Chapter VII Proposition 2.2]; see also Katz & Mazur [26, Theorem 2.3.2]. If $\mathcal{E}$ is given by a Weierstraß Equation (1.3), then in terms of the local parameter $t = -x/y$, y can be expressed in the form $y = -1/w(t)$ for some power series $w(t) \in \Bbbk[[t]]$ satisfying

$$w(t) \equiv t^3 \bmod (t^4).$$

By Equation (4.1), the assignment

$$t \longmapsto \left(\frac{t}{w(t)}, \frac{-2}{w(t)}\right)$$

extends to a $\Bbbk$-algebra homomorphism

$$\Bbbk[[t]]/([p^n]_{F_{\mathcal{E}}}(t)) \longrightarrow \mathcal{E}(\Bbbk[[t]]/(t^{p^{nh}})$$

where h is the height of $F_{\mathcal{E}}$, known to be 1 when $\mathcal{E}$ is an ordinary curve or 2 when it is supersingular. This induces a homomorphism of $\Bbbk$-schemes

$$\mathcal{E}(\Bbbk[[t]]/(t^{p^{nh}})[p^n] \cong \ker[p^n]_{F_{\mathcal{E}}}$$

and Silverman's argument applied to the complete local ring $R = \Bbbk[[t]]/(t^{p^{nh}})$ shows this to be an isomorphism.

An alternative approach to proving this makes use of the Serre-Tate theory described in Katz [24, Theorem 1.2.1], together with Silverman [37, Chapter VII Proposition 2.2]. $\square$

We can now define the *Tate module* of the supersingular elliptic curve $\mathcal{E}$ to be

$$\mathcal{T}_p\mathcal{E} = \mathrm{M}(\mathcal{E}[p^\infty]) \cong \mathrm{M}(\ker[p^\infty]_{F_\mathcal{E}}).$$

Proposition 4.4. *The Tate module $\mathcal{T}_p\mathcal{E}$ is a free topological $\mathbb{W}(\Bbbk)$-module of rank 2.*

In its strongest form, the following result from [42] is due to J. Tate, although never formally published by him; weaker variants were established earlier by Weil and others; a proof appears in [43].

Theorem 4.5. *Let $\mathcal{E}$ and $\mathcal{E}'$ be elliptic curves over $\mathbb{F}_{p^d}$. Then the natural map*

$$\mathrm{Hom}_{\mathbb{F}_{p^d}}(\mathcal{E},\mathcal{E}') \longrightarrow \mathrm{Hom}_{\mathbb{D}_{\mathbb{F}_{p^d}}}(\mathcal{T}_p\mathcal{E}',\mathcal{T}_p\mathcal{E})$$

is injective and the induced map

$$\mathrm{Hom}_{\mathbb{F}_{p^d}}(\mathcal{E},\mathcal{E}')\otimes\mathbb{Z}_p \longrightarrow \mathrm{Hom}_{\mathbb{D}_{\mathbb{F}_{p^d}}}(\mathcal{T}_p\mathcal{E}',\mathcal{T}_p\mathcal{E})$$

is an isomorphism.

Since $\mathrm{Hom}_{\mathbb{F}_{p^d}}(\mathcal{E},\mathcal{E}')$ is a free abelian group of finite rank, $\mathrm{Hom}_{\mathbb{F}_{p^d}}(\mathcal{E},\mathcal{E}')\otimes\mathbb{Z}_p$ agrees with its p-adic completion $\mathrm{Hom}_{\mathbb{F}_{p^d}}(\mathcal{E},\mathcal{E}')\widehat{{}_p}$. This finiteness also implies that for sufficiently large d,

$$\mathrm{Hom}_{\mathbb{F}_{p^d}}(\mathcal{E},\mathcal{E}') = \mathrm{Hom}_{\overline{\mathbb{F}}_p}(\mathcal{E},\mathcal{E}').$$

So interpreting $\mathbb{F}_{p^\infty}$ as $\overline{\mathbb{F}}_p$, Theorem 4.5 also holds in that case.

The above definition of $\mathcal{T}_p\mathcal{E}$ is different in essence from that of the Tate modules

$$\mathcal{T}_\ell\mathcal{E} = \varprojlim_n \mathcal{E}[\ell^n]$$

for primes $\ell \neq p$. However, for any $\Bbbk$-algebra S, we may follow Fontaine [19, Chapitre V] and consider

$$\mathcal{T}'_p\mathcal{E}(S) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \mathcal{E}[p^\infty](S)).$$

In his notation and terminology, Fontaine shows that the functor $\mathcal{T}'_p\mathcal{E}$ satisfies

$$\mathcal{T}'_p\mathcal{E}(S) = \mathrm{Hom}^{\mathrm{cont}}_{\mathbb{D}_\Bbbk}(\mathbb{Q}_p/\mathbb{Z}_p \underset{\mathbb{Z}_p}{\otimes} \mathcal{T}_p\mathcal{E}[p^\infty](S), \mathrm{CW}_\Bbbk(S)).$$

From this it can be deduced that the case $\ell = p$ of the following result holds, the case where $\ell \neq p$ being dealt with in [37, 22].

Theorem 4.6. *Let $\mathcal{E}$ and $\mathcal{E}'$ be elliptic curves over $\mathbb{F}_{p^d}$ and for a prime ℓ let*

$$\mathcal{T}'_\ell\mathcal{E} = \begin{cases} \varprojlim_n \mathcal{E}[\ell^n] & \textit{if } \ell \neq p, \\ \mathcal{T}'_p\mathcal{E} & \textit{if } \ell = p. \end{cases}$$

Then the natural map

$$\mathrm{Hom}_{\mathbb{F}_{p^d}}(\mathcal{E},\mathcal{E}') \longrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{p^d})}(\mathcal{T}'_\ell\mathcal{E},\mathcal{T}'_\ell\mathcal{E}')$$

is injective and the induced map

$$\mathrm{Hom}_{\mathbb{F}_{p^d}}(\mathcal{E},\mathcal{E}')\otimes\mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{p^d})}(\mathcal{T}'_\ell\mathcal{E},\mathcal{T}'_\ell\mathcal{E}')$$

is an isomorphism.

If $\mathcal{E}$ is a supersingular elliptic curve defined over $\overline{\mathbb{F}}_p$, its absolute endomorphism ring $\mathrm{End}\,\mathcal{E} = \mathrm{End}_{\overline{\mathbb{F}}_p}\mathcal{E}$ is a maximal order in a quaternion division algebra over $\mathbb{Q}$. On passing to the p-adic completion of $\mathrm{End}\,\mathcal{E}$, we obtain a non-commutative $\mathbb{W}(\mathbb{F}_{p^2})$-algebra of rank 2,

$$\mathcal{O}_\mathcal{E} = \mathrm{End}\,\mathcal{E}\otimes\mathbb{Z}_p.$$

Proposition 4.7. *The division algebra* $\operatorname{End}\mathcal{E}\otimes\mathbb{Q}$ *is unramified except at* p *and* ∞.

If $\mathcal{E}$ *is defined over* $\mathbb{F}_{p^d}$*, then as a* $\mathbb{W}(\mathbb{F}_{p^2})$*-algebra, the* p*-adic completion* $\mathcal{O}_{\mathcal{E}}$ *is given by*

$$\mathcal{O}_{\mathcal{E}} = \mathbb{W}(\mathbb{F}_{p^2})\left\langle \mathrm{Fr}^{(d)}\right\rangle,$$

where $\mathrm{Fr}^{(d)}$ *is the relative Frobenius map* $\mathrm{Fr}^{(d)}\colon \mathcal{E}\longrightarrow\mathcal{E}^{(p^d)}$ *which satisfies the relations*

$$\begin{cases} {\mathrm{Fr}^{(d)}}^2 = up^d & \text{with } u \text{ a unit in } \mathbb{W}(\mathbb{F}_{p^2}),\\ \mathrm{Fr}^{(d)}\,\alpha = \alpha^{(p^d)}\,\mathrm{Fr}^{(d)} & \text{for all } \alpha\in\mathbb{W}(\mathbb{F}_{p^2}). \end{cases}$$

When $d=1$*,* $\mathcal{O}_{\mathcal{E}} = \mathbb{W}(\mathbb{F}_{p^2})\langle \mathrm{S}\rangle$ *is also isomorphic to the* $\mathbb{W}(\mathbb{F}_{p^2})$*-algebra* $\mathbb{D}_{\mathbb{F}_{p^2}}$ *with* S *corresponding to the Frobenius element* F *and agreeing with* Fr *up to a unit in* $\mathbb{W}(\mathbb{F}_{p^2})$.

Proof. See [42, Chapters 2 & 4]. □

Notice that $\mathcal{O}_{\mathcal{E}}$ has a natural p-adic topology extending that of $\mathbb{Z}_p$. Moreover, every element $\alpha\in\mathcal{O}_{\mathcal{E}}$ has a unique Teichmüller expansion

$$\alpha = \alpha_0 + \alpha_1 S \quad (\alpha_0\in\mathbb{W}(\mathbb{F}_{p^2}),\ \alpha_0^{p^2}=\alpha_0). \tag{4.2}$$

As consequence of Proposition 4.7, the formal group law $F_{\underline{\mathcal{E}}}$ becomes a *formal* $\mathbb{W}(\mathbb{F}_{p^2})$*-module* as defined in Hazewinkel [20]. We set

$$\operatorname{End} F_{\underline{\mathcal{E}}} = \operatorname{End}_{\overline{\mathbb{F}}_p} F_{\underline{\mathcal{E}}}.$$

Proposition 4.8. *The natural homomorphism* $\operatorname{End}\mathcal{E}\longrightarrow\operatorname{End}F_{\underline{\mathcal{E}}}$ *extends to an isomorphism of* $\mathbb{W}(\mathbb{F}_{p^2})$*-algebras* $\mathcal{O}_{\mathcal{E}}\longrightarrow\operatorname{End}F_{\underline{\mathcal{E}}}$.

Proof. The extension to a map on the p-adic completion is straightforward, and the fact that the resulting map is an isomorphism uses Lemma 4.3 together with Tate's Theorem 4.5; see also Katz [23, §IV]. □

Corollary 4.9. $\mathcal{T}_p\mathcal{E}$ *is a module over the* $\mathbb{Z}_p$*-algebra* $(\mathbb{W}(\overline{\mathbb{F}}_p)\underset{\mathbb{Z}_p}{\otimes}\mathbb{W}(\mathbb{F}_{p^2}))\langle \mathrm{S}\rangle$ *in which*

$$\mathrm{S}(\alpha\otimes\beta) = \alpha^{(p)}\otimes\beta^{(p)}\mathrm{S}.$$

Proof. Elements of $\mathbb{W}(\mathbb{F}_{p^2})\subseteq\operatorname{End}\mathcal{E}$ induce morphisms of $\mathcal{T}_p\mathcal{E}$. By definition of the Frobenius operation F in [17, Chapter III §5], we obtain the stated intertwining formula. □

Using Corollary 4.9, we can deduce more on the structure of $\mathcal{T}_p\mathcal{E}$. Let $\Gamma=\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)\cong\widehat{\mathbb{Z}}$ and $\mathrm{H}=\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{p^2})$, hence $\Gamma/\mathrm{H}\cong\mathbb{Z}/2$. By [19, Chapitre III Proposition 2.1] extended in the obvious way to the infinite dimensional situation, the multiplication map

$$\mathbb{W}(\overline{\mathbb{F}}_p)\underset{\mathbb{W}(\mathbb{F}_{p^2})}{\otimes}(\mathcal{T}_p\mathcal{E})^{\mathrm{H}}\longrightarrow\mathcal{T}_p\mathcal{E}$$

is an isomorphism of $\mathbb{W}(\overline{\mathbb{F}}_p)$-modules. Indeed it is an isomorphism of (topological) left Γ-modules and indeed of $\mathbb{W}(\overline{\mathbb{F}}_p)\underset{\mathbb{Z}_p}{\otimes}\mathbb{W}(\mathbb{F}_{p^2})$-modules. Moreover, viewed as a module over the right hand factor of

$$\mathbb{W}(\mathbb{F}_{p^2})\cong 1\underset{\mathbb{Z}_p}{\otimes}\mathbb{W}(\mathbb{F}_{p^2})\subseteq\mathbb{W}(\overline{\mathbb{F}}_p)\underset{\mathbb{Z}_p}{\otimes}\mathbb{W}(\mathbb{F}_{p^2})$$

it is free of rank 2. We can now deduce from this that for any pair of supersingular elliptic curves $\mathcal{E},\mathcal{E}'$, $\operatorname{Hom}_{\mathbb{D}_{\mathbb{F}_{p^d}}}(\mathcal{T}_p\mathcal{E}',\mathcal{T}_p\mathcal{E})$ is a free module of rank 1 over $\mathbb{W}(\mathbb{F}_{p^2})\langle\mathrm{S}\rangle$, hence it is a free module of rank 2 over $\mathbb{W}(\mathbb{F}_{p^2})$.

The ring $\mathbb{W}(\mathbb{F}_{p^2})\langle \mathrm{S}\rangle$ is familiar to topologists as the absolute endomorphism ring of the universal Lubin-Tate formal group law height 2, agreeing with that of the natural orientation in Morava $K(2)$-theory. Its group of units is

$$\mathbb{S}_2 = \{\alpha_0 + \alpha_1 \mathrm{S} \in \mathbb{W}(\mathbb{F}_{p^2})\langle \mathrm{S}\rangle : \alpha_0, \alpha_1 \in \mathbb{W}(\mathbb{F}_{p^2}),\ \alpha_0 \not\equiv 0 \bmod (p)\},$$

while

$$\mathbb{S}_2^0 = \{\alpha_0 + \alpha_1 \mathrm{S} \in \mathbb{W}(\mathbb{F}_{p^2})\langle \mathrm{S}\rangle : \alpha_0, \alpha_1 \in \mathbb{W}(\mathbb{F}_{p^2}),\ \alpha_0 \equiv 1 \bmod (p)\}$$

is its group of *strict units*, known to topologists as the *Morava stabilizer group*. Let $\mathbb{B}_2$ be the rationalization of $\mathbb{W}(\mathbb{F}_{p^2})\langle \mathrm{S}\rangle$ which is a 4-dimensional central division algebra over $\mathbb{Q}_p$. Adopting notation of [8], we will also introduce the following closed subgroup of the group of units $\widetilde{\mathbb{S}}_2 = \mathbb{B}_2^\times$:

$$\widetilde{\mathbb{S}}_2^0 = \bigcup_{r\in\mathbb{Z}} \mathbb{S}_2^0\, \mathrm{S}^r.$$

Notice also that

$$\widetilde{\mathbb{S}}_2 = \bigcup_{r\in\mathbb{Z}} \mathbb{S}_2\, \mathrm{S}^r.$$

Then $\mathbb{S}_2 \lhd \widetilde{\mathbb{S}}_2$ and $\mathbb{S}_2^0 \lhd \widetilde{\mathbb{S}}_2^0$, *i.e.*, these are closed normal subgroups.

We can rationalize the Tate module $\mathcal{T}_p\mathcal{E}$, to give

$$\mathcal{V}_p\mathcal{E} = \mathbb{Q}_p \underset{\mathbb{Z}_p}{\otimes} \mathcal{T}_p\mathcal{E},$$

which is a 2-dimensional vector space over the fraction field $\mathrm{B}(\Bbbk) = \mathbb{Q}_p \underset{\mathbb{Z}_p}{\otimes} \mathbb{W}(\Bbbk)$. In fact, $\mathcal{V}_p\mathcal{E}$ is a module over the rationalization $\mathbb{B}_\Bbbk = \mathbb{Q}_p \underset{\mathbb{Z}_p}{\otimes} \mathbb{D}_\Bbbk$. We can generalize Tate's Theorem to give the following, which we only state for curves defined over $\overline{\mathbb{F}}_p$.

Theorem 4.10. *Let $\underline{\mathcal{E}_1}$ and $\underline{\mathcal{E}_2}$ be elliptic curves over $\overline{\mathbb{F}}_p$. Then the natural map*

$$\mathbf{Isog}^\times(\underline{\mathcal{E}_1}, \underline{\mathcal{E}_2}) \longrightarrow \mathrm{Hom}_{\mathbb{B}_{\overline{\mathbb{F}}_p}}(\mathcal{V}_p\mathcal{E}_2, \mathcal{V}_p\mathcal{E}_1)$$

is injective and has image contained in $\mathrm{InvtHom}_{\mathbb{B}_{\overline{\mathbb{F}}_p}}(\mathcal{V}_p\mathcal{E}_2, \mathcal{V}_p\mathcal{E}_1)$*, the open subset of invertible homomorphisms, and the induced map*

$$\mathbf{Isog}^\times(\underline{\mathcal{E}_1}, \underline{\mathcal{E}_2})\widehat{\ }_p \longrightarrow \mathrm{InvtHom}_{\mathbb{B}_{\overline{\mathbb{F}}_p}}(\mathcal{V}_p\mathcal{E}_2, \mathcal{V}_p\mathcal{E}_1)$$

is a homeomorphism.

The natural map

$$\mathbf{SepIsog}^\times(\underline{\mathcal{E}_1}, \underline{\mathcal{E}_2}) \longrightarrow \mathrm{Hom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}_2, \mathcal{T}_p\mathcal{E}_1)$$

is injective with image contained in the open set of invertible homomorphisms and the induced map

$$\mathbf{SepIsog}^\times(\underline{\mathcal{E}_1}, \underline{\mathcal{E}_2})\widehat{\ }_p \longrightarrow \mathrm{InvtHom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}_2, \mathcal{T}_p\mathcal{E}_1)$$

is a homeomorphism.

Similar results hold for the supersingular isogeny categories.

Every separable isogeny induces an isomorphism of Tate modules, therefore the image of $\mathbf{SepIsog}(\mathcal{E}_1, \mathcal{E}_2)$ in $\mathrm{Hom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}_2, \mathcal{T}_p\mathcal{E}_1)$ is a dense subset of $\mathrm{InvtHom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}_2, \mathcal{T}_p\mathcal{E}_1)$.

Notice also that $\alpha \in \mathrm{InvtHom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}, \mathcal{T}_p\mathcal{E})$ with $\alpha = \alpha_0 + \alpha_1 S$ as in Equation (4.2), has the well defined effect $\alpha^*\omega = \alpha_0\omega$ on 1-forms, since this is certainly true for elements of the dense subgroup $\mathrm{End}\,\mathcal{E}^\times \subseteq \mathrm{InvtHom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}, \mathcal{T}_p\mathcal{E})$.

Theorem 4.10 leads us to define the following 'thickenings' of our isogeny categories. Starting with the category **Isog** and its subcategories, we enlarge each to a subcategory of $\widetilde{\mathbf{Isog}}$, with the same objects but as the set of morphisms $\mathcal{E}_1 \longrightarrow \mathcal{E}_2$,

$$\widetilde{\mathbf{Isog}}(\mathcal{E}_1, \mathcal{E}_2) = \mathrm{Hom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}_2, \mathcal{T}_p\mathcal{E}_1) - \{0\},$$
$$\widetilde{\mathbf{Isog}}^{\times}(\mathcal{E}_1, \mathcal{E}_2) = \mathrm{InvtHom}_{\mathbb{B}_{\overline{\mathbb{F}}_p}}(\mathcal{V}_p\mathcal{E}_2, \mathcal{V}_p\mathcal{E}_1),$$
$$\widetilde{\mathbf{SepIsog}}^{\times}(\mathcal{E}_1, \mathcal{E}_2) = \mathrm{InvtHom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}_2, \mathcal{T}_p\mathcal{E}_1),$$

and similarly for the supersingular categories.

We can make similar constructions for the categories whose objects are oriented elliptic curves, setting

$$\widetilde{\mathbf{SepIsog}}^{\times}((\mathcal{E}_1, \omega_1), (\mathcal{E}_2, \omega_2)) = \mathrm{InvtHom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}_2, \mathcal{T}_p\mathcal{E}_1),$$

and if $\mathcal{E}_1, \mathcal{E}_2$ are supersingular,

$$\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}((\mathcal{E}_1, \omega_1), (\mathcal{E}_2, \omega_2)) = \mathrm{InvtHom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}_2, \mathcal{T}_p\mathcal{E}_1).$$

These morphism sets all have a natural profinite topologies, and composition of morphisms is continuous. These categories are 'formal schemes' in the sense of Devinatz [18] and Strickland [38] and we will make use of this in Section 7. Their object sets have the form $\mathrm{Spec}_{\overline{\mathbb{F}}_p} {}^{\mathrm{ss}}E\ell\ell_*$, while the morphism set of a pair of objects can be identified with the limit of the pro-system obtained by factoring out by the open neighbourhoods of the identity morphisms in the sets of homomorphisms between the associated Tate modules. For example,

$$\widetilde{\mathbf{Isog}}(\mathcal{E}_1, \mathcal{E}_2) = \lim_{\overleftarrow{U}} \mathrm{Hom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}_2, \mathcal{T}_p\mathcal{E}_1/U),$$

where the limit is taken over the basic neighbourhoods U of 0 in $\mathcal{T}_p\mathcal{E}_1$ which are just the finite index subgroups. We can describe representing algebras for some of these formal schemes. We will do this for the supersingular category $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$. Recall Theorem 3.5.

Theorem 5.1. *There is an equivariant isomorphism of topological groupoids with $\mathbb{G}_{\mathrm{m}}$-action,*

$$\mathrm{Spec}^{\mathrm{f}}_{\overline{\mathbb{F}}_p} \overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma_* \cong \widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}.$$

Moreover, $\overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma_{2n}$ can be identified with the set of all continuous functions $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}} \longrightarrow \overline{\mathbb{F}}_p$ of weight n and ${}^{\mathrm{ss}}\Gamma_{2n} \subseteq \overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma_{2n}$ can be identified with the subset of Galois invariant functions.

Proof. This follows from an argument similar to that of [2]; see also [7] for a similar generalization. The idea is to consider locally constant functions

$$\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}((\mathcal{E}_1, \omega_1), (\mathcal{E}_2, \omega_2)) \cong \mathbb{W}(\mathbb{F}_{p^2})\langle \mathrm{S} \rangle \longrightarrow \overline{\mathbb{F}}_p,$$

where $(\mathcal{E}_1, \omega_1)$, $(\mathcal{E}_2, \omega_2)$ are two elliptic curves. The space of all such functions is determined using the ideas of [2], and turns out to be spanned by monomials in generalized Teichmüller functions relative to expansions in terms of powers of S. Up to powers of u, these Teichmüller functions are the images under the natural map $E\ell\ell_*E\ell\ell \longrightarrow \overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma_{2n}$ of the elements $D_r \in E\ell\ell_*E\ell\ell$ of [6, equation (9.8)]. $\square$

For later use we provide a useful example of such a Galois invariant continuous function on $\mathbf{SepIsog}_{\mathrm{ss}}^{\times}$, namely

$$\text{(5.1)} \qquad \operatorname{ind}\colon \widetilde{\mathbf{SepIsog}_{\mathrm{ss}}^{\times}} \longrightarrow \overline{\mathbb{F}}_p; \quad \operatorname{ind}((\mathcal{E},\omega) \xrightarrow{\varphi} (\mathcal{E}',\omega')) = \deg\varphi \bmod (p),$$

where $\deg\varphi \bmod (p)$ is calculated by choosing a separable isogeny $\varphi_0\colon (\mathcal{E},\omega) \longrightarrow (\mathcal{E}',\omega')$ which approximates φ in $\operatorname{Hom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p\mathcal{E}', \mathcal{T}_p\mathcal{E})$ in the sense that $\varphi \equiv \varphi_0 \bmod (S)$. Clearly ind is locally constant, hence continuous, as well as Galois invariant. Also, for a composable pair of morphisms φ, θ,

$$\operatorname{ind}(\varphi\theta) = \operatorname{ind}(\varphi)\operatorname{ind}(\theta).$$

Proposition 5.2. *The function* ind *corresponds to a element of* ${}^{\mathrm{ss}}\Gamma_0$ *which is group-like under the coaction* ψ *and antipode* χ *in the sense that*

$$\psi(\mathrm{ind}) = \mathrm{ind}\otimes\mathrm{ind}, \quad \chi(\mathrm{ind}) = \mathrm{ind}^{-1}.$$

6. Continuous cohomology of profinite groupoids

The results of this section appeared in greater detail in [12].

Let $\mathcal{G}$ be a groupoid, *i.e.*, a small category in which every morphism is invertible. The function $\operatorname{Obj}\mathcal{G} \longrightarrow \operatorname{Mor}\mathcal{G}$ which sends each object to its identity morphism embeds $\operatorname{Obj}\mathcal{G}$ into $\operatorname{Mor}\mathcal{G}$ so we can view $\mathcal{G}$ as consisting of the set of all its morphisms. We will use the notation

$$\mathcal{G}(*,x) = \bigcup_{y\in\operatorname{Obj}\mathcal{G}} \mathcal{G}(y,x) \subseteq \mathcal{G}.$$

Following Higgins [21] we define a subgroupoid $\mathcal{N}$ of a groupoid $\mathcal{G}$ to be *normal* if it satisfies the following conditions:
A) $\operatorname{Obj}\mathcal{N} = \operatorname{Obj}\mathcal{G}$;
B) for every morphism $x \xrightarrow{f} y$ in $\mathcal{G}$,

$$f\mathcal{N}(x,x)f^{-1} = \mathcal{N}(x,x).$$

We will write $\mathcal{N} \lhd \mathcal{G}$ if $\mathcal{N}$ is a normal subgroupoid of $\mathcal{G}$. When $\mathcal{N} \lhd \mathcal{G}$ we can form the *quotient groupoid* $\mathcal{G}/\mathcal{N}$ whose objects are equivalence classes of objects of $\mathcal{G}$ under the relation $\sim$ for which

$$x \sim y \iff \exists\, x \xrightarrow{h} y \text{ in } \mathcal{N},$$

and whose morphisms are equivalence classes of morphisms under the relation

$$x \xrightarrow{f} y \sim x' \xrightarrow{f'} y' \iff \exists\, x \xrightarrow{p} x',\ y \xrightarrow{q} y' \text{ in } \mathcal{N} \text{ s.t. } f' = qfp^{-1}.$$

Whenever two classes contain composable elements, composition of equivalence classes can be defined by

$$[y \xrightarrow{g} z][x \xrightarrow{f} y] = [x \xrightarrow{gf} z],$$

which is well defined since for morphisms $x \xrightarrow{p} x'$, $y \xrightarrow{q} y'$, $y \xrightarrow{r} y'$, $z \xrightarrow{s} z'$,

$$(sgr^{-1})(qfp^{-1}) = sg(r^{-1}q)fp^{-1} = (sh)gfp^{-1}$$

where $h = g(r^{-1}q)g^{-1}$ is in $\mathcal{N}(z,z)$. There is a quotient functor $\mathcal{G} \longrightarrow \mathcal{G}/\mathcal{N}$.

We define a groupoid $\mathcal{G}$ to be *automorphism finite* if for every $x \in \operatorname{Obj}\mathcal{G}$, $\mathcal{G}(x,x)$ is a finite group. We define a groupoid $\mathcal{G}$ to be (*automorphism*) *profinite* if it is the inverse limit of automorphism finite groupoids,

$$\mathcal{G} \cong \varprojlim_{\mathcal{N}\lhd\mathcal{G}} \mathcal{G}/\mathcal{N}.$$

Such a groupoid has a natural topology in which the basic open sets have the form

$$U(x \xrightarrow{f} y, \mathcal{N}) = \{x \xrightarrow{g} y : gf^{-1} \in \mathcal{N}(y,y)\},$$

where $f \in \operatorname{Mor}\mathcal{G}$ and $\mathcal{G}/\mathcal{N}$ is automorphism finite.

A *topological groupoid* is a groupoid which is a topological space such that the partial composition $\mathcal{G} \underset{\operatorname{Obj}\mathcal{G}}{\times} \mathcal{G} \longrightarrow \mathcal{G}$, inverse function $\mathcal{G} \longrightarrow \mathcal{G}$, domain and codomain functions $\mathcal{G} \longrightarrow \operatorname{Obj}\mathcal{G}$ are all continuous, where $\operatorname{Obj}\mathcal{G}$ has the subspace topology. A profinite groupoid in the above sense is a topological groupoid.

A groupoid $\mathcal{G}$ is *connected* if for every pair of objects x, y in $\mathcal{G}$ there is a morphism $x \xrightarrow{f} y$. More generally, $\mathcal{G}$ is the disjoint union of its *connected components* which are the connected subgroupoids.

In order to define the cohomology of profinite groupoids we first need to define suitable a notion of module, and we follow the ideas of Galois cohomology, accessibly described in Shatz [36], with Weibel [44] providing a more general cohomological discussion.

For a profinite groupoid $\mathcal{G}$, a *proper $\mathcal{G}$-module* (over a commutative unital ring $\Bbbk$) is a functor $\underline{M}\colon \mathcal{G} \longrightarrow \mathbf{Mod}_{\Bbbk}$ in which for $x, y \in \operatorname{Obj}\mathcal{G}$, $m \in \underline{M}(x)$, $f \in \mathcal{G}(x,y)$, the set

$$\operatorname{Stab}_{\mathcal{G}}(m, f, y) = \{g \in \mathcal{G}(x,y) : \underline{M}(g)m = \underline{M}(f)m\} \subseteq \mathcal{G}(x,y)$$

is open. This generalizes the notion of proper module for a profinite group, for which stabilizers of points are of finite index. We will denote the category of all proper $\mathcal{G}$-modules over $\Bbbk$ by $\mathbf{Mod}_{\Bbbk,\mathcal{G}}$, where the morphisms are natural transformations.

We set

$$\underline{\mathbf{M}} = \prod_{x \in \operatorname{Obj}\mathcal{G}} \underline{M}(x)$$

and view this as a discrete topological space. We define a *section* of $\underline{M}$ to be a function $\Phi\colon \operatorname{Obj}\mathcal{G} \longrightarrow \underline{\mathbf{M}}$ such that

$$\Phi(x) \in \underline{M}(x) \quad (x \in \operatorname{Obj}\mathcal{G}).$$

We will denote the $\Bbbk$-module of all sections by $\operatorname{Sect}(\mathcal{G}; \underline{M})$.

Proposition 6.1. *Let $\mathcal{G}$ be a profinite groupoid and $\Bbbk$ a commutative unital ring.*

a) $\mathbf{Mod}_{\Bbbk,\mathcal{G}}$ *is an abelian category with structure inherited from that of* $\mathbf{Mod}_{\Bbbk}$*.*
b) $\mathbf{Mod}_{\Bbbk,\mathcal{G}}$ *has sufficiently many injectives.*

Proof. These are straightforward generalizations of the analogous results for profinite groups found in [36]; further details appear in [12]. □

We will consider two functors $\mathbf{Mod}_{\Bbbk,\mathcal{G}} \longrightarrow \mathbf{Mod}_{\Bbbk}$. The first is a sort of fixed point construction

$$(\ )^{\mathcal{G}}\colon \underline{M} \rightsquigarrow \underline{M}^{\mathcal{G}} = \{\Phi \in \operatorname{Sect}(\mathcal{G}; \underline{M}) : \forall f \in \mathcal{G},\ \underline{M}(f)(\Phi(\operatorname{dom} f)) = \Phi(\operatorname{codom} f)\}.$$

This functor is left exact, so it has right derived functors $\mathrm{R}^n(\ )^{\mathcal{G}}$ for $n \geqslant 0$ which can be viewed as the continuous cohomology of $\mathcal{G}$, $\mathrm{H}^n_c(\mathcal{G};\ )$.

For $x_0 \in \operatorname{Obj}\mathcal{G}$, we define a kind of 'localization at x_0',

$$(\ )_{x_0}\colon \underline{M} \rightsquigarrow \underline{M}(x_0)^{\mathcal{G}(x_0,x_0)},$$

obtained by restricting to $\underline{M}(x_0)$ and taking the fixed points under the action of the automorphism group of x_0. This is left exact and has right derived functors $\mathrm{R}^n(\ )_{x_0}$ which we will denote by $\mathrm{H}^n_{x_0}(\mathcal{G};\ )$.

Proposition 6.2. *If the profinite groupoid $\mathcal{G}$ is connected, then for any $x_0 \in \operatorname{Obj}\mathcal{G}$, there is a natural equivalence of functors*

$$(\ )_{x_0} \cong (\ )^{\mathcal{G}}.$$

Hence there are natural equivalences of functors

$$\mathrm{H}^n_c(\mathcal{G};\ ) \cong \mathrm{H}^n_{x_0}(\mathcal{G};\ ) \quad (n \geqslant 0).$$

Proof. For the first part, we produce a $\Bbbk$-isomorphism $F\colon \underline{M}_{x_0} \xrightarrow{\cong} \underline{M}^{\mathcal{G}}$. For $m \in \underline{M}_{x_0}$, define $F(m) = \Phi_m$ by

$$\Phi_m(x) = \underline{M}(f)m \quad (x \in \operatorname{Obj}\mathcal{G})$$

where we choose *any* $f \in \mathcal{G}(x_0, x)$; this choice does not affect the outcome since for a second choice $g \in \mathcal{G}(x_0, x)$, $f^{-1}g \in \mathcal{G}(x_0, x_0)$ and therefore

$$\underline{M}(g)m = \underline{M}(f)\underline{M}(f^{-1}g)m = \underline{M}(f)m.$$

This is easily verified to be an isomorphism.

The second part follows using a standard result on δ-functors described in [44, chapter 2]. □

This result shows that the calculation of the continuous cohomology $\mathrm{H}^*_c(\mathcal{G}; \underline{M})$ of a proper module $\underline{M}$ reduces to continuous group cohomology.

Theorem 6.3. *If $\mathcal{G}$ is a connected profinite groupoid and $\underline{M}$ is a proper $\mathcal{G}$-module over $\Bbbk$, then for any $x_0 \in \operatorname{Obj}\mathcal{G}$,*

$$\mathrm{H}^*_c(\mathcal{G}; \underline{M}) \cong \mathrm{H}^*_c(\mathcal{G}(x_0, x_0); \underline{M}(x_0)).$$

In the general case we have the following.

Theorem 6.4. *If $\mathcal{G}$ is a profinite groupoid and $\underline{M}$ is a proper $\mathcal{G}$-module over $\Bbbk$, then for each $n \geqslant 0$,*

$$\mathrm{H}^n_c(\mathcal{G}; \underline{M}) \cong \prod_C \mathrm{H}^n_c(\mathcal{G}(x_C, x_C); \underline{M}(x_C)),$$

where C ranges over the connected components of $\mathcal{G}$ and x_C is a chosen object of C.

Remark 6.5. The familiar approach to proving results of this kind would require there to be a topological splitting of $\mathcal{G}$ as $\operatorname{Obj}\mathcal{G} \rtimes \mathcal{G}(x_0, x_0)$. Indeed, in our application no such continuous splitting exists and we would need to pass to a quotient category to make use of such an argument.

Remark 6.6. The fixed point functor $(\ )^{\mathcal{G}}$ agrees with the limit over the category $\mathcal{G}$, hence the continuous cohomology functors $\mathrm{H}^n_c(\mathcal{G};\ )$ are the derived functors of the limit. This connects our work with recent results of Hopkins, Mahowald *et al.* on the spectra EO_2 and TMF, the ring of topological modular forms.

7. On the cohomology of topological Hopf algebroids

The best reference for the following material is Devinatz [18] which contains the most thorough discussion we are aware of on the continuous cohomology of topological groupoid schemes of the type under consideration in this paper. We simply sketch the required details from [18, §1], amending them slightly to suit our needs. An alternative perspective on the cohomology of categories is provided by Baues & Wirsching [13].

Let $\mathcal{C}$ be a groupoid, $\Bbbk$ a commutative unital ring. Then $\mathbf{Mod}^{\mathrm{c}}_{\Bbbk}$ will denote the category of *complete Hausdorff $\Bbbk$-modules* defined in [18, Definition 1.1]. Similarly, $\mathbf{Alg}^{\mathrm{c}}_{\Bbbk}$ will denote the category of *complete commutative $\Bbbk$-algebras*. We will refer to morphisms in these two categories as *continuous homomorphisms* of complete modules or algebras.

A *cogroupoid object* in $\mathbf{Alg}^{\mathrm{c}}_{\Bbbk}$ is then a pair (A,Γ) of objects in $\mathbf{Alg}^{\mathrm{c}}_{\Bbbk}$ together with the usual structure maps $\eta_R,\eta_L,\varepsilon,\psi,\chi$ for a Hopf algebroid over $\Bbbk$ except that in all relevant diagrams the completed tensor product $\underset{\Bbbk}{\widehat{\otimes}}$ has to be used; such data $(A,\Gamma,\eta_R,\eta_L,\varepsilon,\psi,\chi)$ will be referred to as constituting a *complete topological Hopf algebroid*. Equivalently, $\mathcal{C}=\mathrm{Spec}^{\mathrm{f}}_{\Bbbk}\,\Gamma$ is an (affine) *formal groupoid scheme*.

We can also consider the category $\mathbf{Comod}^{\mathrm{c}}_{\Gamma}$ of complete (left) Γ-comodules with morphisms being comodule morphisms also lying in $\mathbf{Mod}^{\mathrm{c}}_{\Bbbk}$. For two objects M, N in $\mathbf{Comod}^{\mathrm{c}}_{\Gamma}$, we will denote the set of morphisms $M\longrightarrow N$ by $\mathrm{Hom}_{\Gamma}(M,N)$. The functor

$$\mathbf{Comod}^{\mathrm{c}}_{\Gamma}\longrightarrow\mathbf{Mod}_{\Bbbk};\quad M\rightsquigarrow\mathrm{Hom}_{\Gamma}(A,M)$$

is left exact and its right derived functors form a graded functor $\mathrm{Ext}^*_{\Gamma}(A,\ )$.

Given a continuous morphism of complete Hopf algebroids $f\colon(A,\Gamma)\longrightarrow(B,\Sigma)$ and a Γ-comodule M, there is an induced map

$$H^*f\colon\ \mathrm{Ext}^*_{\Gamma}(A,M)\longrightarrow\mathrm{Ext}^*_{\Sigma}(B,f^*M)$$

where $f^*M=B\underset{A}{\widehat{\otimes}}M$ has the Σ-comodule structure described in [18].

Now recall from [18, definition 1.14] the notion of a *natural equivalence* $\tau\colon f\longrightarrow g$ between two continuous morphisms $f,g\colon(A,\Gamma)\longrightarrow(B,\Sigma)$ of complete Hopf algebroids. In particular, such a τ induces a continuous homomorphism of complete Σ-comodules $\tau^*\colon g^*M\longrightarrow f^*M$, which in turn induces a map

$$H^*\tau\colon\ \mathrm{Ext}^*_{\Sigma}(B,g^*M)\longrightarrow\mathrm{Ext}^*_{\Sigma}(B,f^*M).$$

We will require Devinatz's important Proposition 1.16.

Proposition 7.1. *Let $\tau\colon f\longrightarrow g$ be a natural equivalence between continuous morphisms $f,g\colon(A,\Gamma)\longrightarrow(B,\Sigma)$ of complete Hopf algebroids. Then for any continuous Γ-comodule M,*

$$H^*(\tau^*)\circ H^*g=H^*f\colon\ \mathrm{Ext}^*_{\Gamma}(A,M)\longrightarrow\mathrm{Ext}^*_{\Sigma}(B,f^*M).$$

Using Devinatz's notion of *equivalence* of two complete Hopf algebroids we can deduce

Corollary 7.2. *If $f\colon(A,\Gamma)\longrightarrow(B,\Sigma)$ is an equivalence of complete Hopf algebroids, then*

$$H^*f\colon\ \mathrm{Ext}^*_{\Gamma}(A,M)\longrightarrow\mathrm{Ext}^*_{\Sigma}(B,f^*M)$$

is an isomorphism.

All of the above can also be reworked with graded $\Bbbk$-modules and $\Bbbk$-algebras. As Devinatz observes, when Γ is concentrated in even degrees, this is equivalent to introducing actions of the multiplicative group scheme $\mathbb{G}_{\mathrm{m}}$ which factor through the quotient scheme $\mathbb{G}_{\mathrm{m}}/\mu_2$ where $\mu_d\subseteq\mathbb{G}_{\mathrm{m}}$ is subscheme of d-th roots of unity. This applies to the situations of interest to us and indeed locally the actions of $\mathbb{G}_{\mathrm{m}}$ factor through $\mathbb{G}_{\mathrm{m}}/\mu_{2n}$ where may take some of the values $n=2,4,6$. An alternative approach to this is to view a $\mathbb{Z}$-graded module as a $\mathbb{Z}/2$-graded view module with action of $\mathbb{G}_{\mathrm{m}}$, and we prefer this approach. We then define an element x in degree n to be of *weight* $\mathrm{wt}x=n/2$; this means that whenever $\alpha\in\mathbb{G}_{\mathrm{m}}$,

$$\alpha\cdot x=\begin{cases}\alpha^{\mathrm{wt}x}x & \text{if } n \text{ even},\\ -\alpha^{\mathrm{wt}x-1}x & \text{if } n \text{ odd}.\end{cases}$$

For a profinite groupoid $\mathcal{G}$ and a commutative unital ring $\Bbbk$ with the discrete topology, the pair of $\Bbbk$-algebras

$$A=\mathrm{Map}^{\mathrm{c}}(\mathrm{Obj}\,\mathcal{G},\Bbbk),\quad\Gamma=\mathrm{Map}^{\mathrm{c}}(\mathcal{G},\Bbbk)$$

form a complete topological Hopf algebroid (A, Γ) with obvious structure maps induced from $\mathcal{G}$. A proper $\mathcal{G}$-module $\underline{M}$ with each $\underline{M}(x)$ finitely generated over $\Bbbk$ is equivalent to a topological Γ-comodule M, where

$$M = \mathrm{Sect}(\mathcal{G}; \underline{M})$$

is a left A-module via

$$(\alpha \cdot \Phi)(x) = \alpha(x)\Phi(x),$$

and the coproduct $\psi \colon M \longrightarrow \Gamma \underset{A}{\otimes} M$ is determined on an element $m \in M$ by an expression of the form

$$\psi(m) = \sum_s \theta_s \otimes m_s,$$

where $m_s \in M$ and $\theta_s \in \Gamma$ so that for each pair of elements $x, y \in \mathrm{Obj}\,\mathcal{G}$, θ_s restricts to a locally constant function on $\mathcal{G}(x, y)$.

8. Connectivity of the category of supersingular isogenies

In this section we will show that the category of isogenies of supersingular elliptic curves $\mathbf{Isog}_{\mathrm{ss}}$ is connected in the sense that there is a morphism between any given pair of objects.

Theorem 8.1. *Two elliptic curves $\mathcal{E}$, $\mathcal{E}'$ defined over a finite field $\mathbb{F}_{p^d}$ are isogenous over $\mathbb{F}_{p^d}$ if and only if $|\mathcal{E}(\mathbb{F}_{p^d})| = |\mathcal{E}'(\mathbb{F}_{p^d})|$.*

Proof. See [22, Chapter 3 Theorem 8.4]. □

Theorem 8.2. *An elliptic curve $\mathcal{E}$ defined over a finite field $\mathbb{F}_{p^d}$ satisfies*

- $|\mathcal{E}(\mathbb{F}_{p^d})| = 1 + p^d$ *if d is odd;*
- $|\mathcal{E}(\mathbb{F}_{p^{2m}})| = (1 \pm p^m)^2$ *if* $\mathrm{End}_{\overline{\mathbb{F}}_p} \mathcal{E} = \mathrm{End}_{\mathbb{F}_{p^d}} \mathcal{E}$.

Proof. The list of all possible orders of $|\mathcal{E}(\mathbb{F}_{p^d})|$ appears in [42], while [34] gives a complete list of the actual groups $\mathcal{E}(\mathbb{F}_{p^d})$ that can occur. □

Theorem 8.3. *The isogeny categories $\mathbf{Isog}_{\mathrm{ss}}$ and $\widetilde{\mathbf{Isog}}_{\mathrm{ss}}$ are connected.*

Proof. We will show that any two supersingular elliptic curves $\mathcal{E}$, $\mathcal{E}'$ defined over $\overline{\mathbb{F}}_p$ are isogenous. We may assume that $\mathcal{E}$ and $\mathcal{E}'$ are both defined over some finite field and then by Theorems 8.1 and 8.2 we need only show that they become isogenous over some larger finite field. We begin by enlarging the common field of definition to $\mathbb{F}_{p^{2m}}$ for which

$$\mathrm{End}_{\overline{\mathbb{F}}_p} \mathcal{E} = \mathrm{End}_{\mathbb{F}_{p^{2m}}} \mathcal{E}, \quad \mathrm{End}_{\overline{\mathbb{F}}_p} \mathcal{E}' = \mathrm{End}_{\mathbb{F}_{p^{2m}}} \mathcal{E}'.$$

Thus $|\mathcal{E}(\mathbb{F}_{p^{2m}})|$ and $|\mathcal{E}'(\mathbb{F}_{p^{2m}})|$ both have the form $(1 \pm p^m)^2$. If these are equal then the curves are isogenous over $\mathbb{F}_{p^{2m}}$. Otherwise we may assume that

$$|\mathcal{E}(\mathbb{F}_{p^{2m}})| = 1 + 2p^m + p^{2m}, \quad |\mathcal{E}'(\mathbb{F}_{p^{2m}})| = 1 - 2p^m + p^{2m}.$$

If the Weierstraß equation of $\mathcal{E}$ is

$$\mathcal{E} \colon y^2 = 4x^3 - ax - b,$$

taking a quadratic non-residue u in $\mathbb{F}_{p^{2m}}$ allows us to define a twisted curve by

$$\mathcal{E}^u \colon y^2 = 4x^3 - u^2ax - u^3b,$$

which becomes isomorphic to $\mathcal{E}$ over $\mathbb{F}_{p^{4m}}$. If

$$N_0 = |\{t \in \mathbb{F}_{p^{2m}} : 4t^3 - at - b = 0\}|,$$
$$N_1 = |\{t \in \mathbb{F}_{p^{2m}} : 4t^3 - at - b \neq 0 \text{ is a quadratic residue}\}|,$$

then

$$1 + N_0 + 2N_1 = 1 + 2p^m + p^{2m}.$$

But as

$$4x^3 - u^2ax - u^3b = u^3(4(u^{-1}x)^3 - a(u^{-1}x) - b),$$

we find that

$$\begin{aligned}|\mathcal{E}^u(\mathbb{F}_{p^{2m}})| &= 1 + N_0 + 2(p^{2m} - N_0 - N_1)\\ &= 1 - N_0 - 2N_1 + 2p^{2m}\\ &= 1 - 2p^m + p^{2m}.\end{aligned}$$

Hence,

$$|\mathcal{E}'(\mathbb{F}_{p^{2m}})| = |\mathcal{E}^u(\mathbb{F}_{p^{2m}})|$$

and so these are isogenous curves over $\mathbb{F}_{p^{2m}}$, implying that $\mathcal{E}'$ is isogenous to $\mathcal{E}$ over $\mathbb{F}_{p^{2m}}$.

We could have also used the fact $j(\mathcal{E}^u) = j(\mathcal{E})$ to obtain an isomorphism $\mathcal{E}^u \cong \mathcal{E}$ over $\overline{\mathbb{F}}_p$, but the argument given is more explicit about the field of definition of such an isomorphism.

The connectivity of $\widetilde{\mathbf{Isog}}_{\mathrm{ss}}$ now follows from Tate's Theorem 4.5. ☐

Corollary 8.4. *The groupoids* $\mathbf{Isog}^{\times}_{\mathrm{ss}}$ *and* $\widetilde{\mathbf{Isog}}^{\times}_{\mathrm{ss}}$ *are connected.*

The following deeper fact about supersingular curves over finite fields, which is a consequence of Theorem A.1, allows us to show the connectivity of $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$.

Theorem 8.5. *For any prime $p > 3$, there is a supersingular elliptic curve $\mathcal{E}_0$ defined over $\mathbb{F}_p$. If $p > 11$, this can be chosen to satisfy $j(\mathcal{E}) \not\equiv 0, 1728 \bmod (p)$.*

Proposition 8.6. *The separable isogeny categories* $\mathbf{SepIsog}^{\times}_{\mathrm{ss}}$ *and* $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ *are connected as are the associated categories of isogenies of oriented elliptic curves* $\mathbf{SepIsog}^{\times}_{\mathrm{ss}}$ *and* $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$*.*

Proof. Choose a supersingular curve $\mathcal{E}_0$ defined over $\mathbb{F}_p$ as in Theorem 8.5. For each supersingular curve $\mathcal{E}$ defined over $\overline{\mathbb{F}}_p$ there is an isogeny $\varphi\colon \mathcal{E} \longrightarrow \mathcal{E}_0$. By Proposition 2.1, there is a factorization

$$\varphi = \mathrm{Fr}^k \circ \varphi_s,$$

where $\varphi_s\colon \mathcal{E} \longrightarrow \mathcal{E}_0^{(1/p^k)}$ is separable. But $\mathcal{E}_0^{(1/p^k)} = \mathcal{E}_0$ since $\mathcal{E}_0$ is defined over $\mathbb{F}_p$, hence $\varphi_s\colon \mathcal{E} \longrightarrow \mathcal{E}_0$ is a separable isogeny connecting $\mathcal{E}$ to $\mathcal{E}_0$. Thus $\mathbf{SepIsog}^{\times}_{\mathrm{ss}}$ is connected.

Now Tate's Theorem 4.5 implies that $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ is connected.

The results for $\mathbf{SepIsog}^{\times}_{\mathrm{ss}}$ and $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ follow by twisting. ☐

These results have immediate implications for the cohomology of the groupoids $\widetilde{\mathbf{Isog}}^{\times}_{\mathrm{ss}}$ and $\mathbf{SepIsog}^{\times}_{\mathrm{ss}}$, however, for our purposes with $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ we need to take the topological structure into account and consider an appropriate continuous cohomology. We will discuss this further in the following sections.

9. Splittings of a quotient of the supersingular category of isogenies

In this section we introduce some quotient categories of $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$. The first is perhaps more 'geometric', while the second is a 'p-typical' approximation.

Our first quotient category is $\boldsymbol{\mathcal{C}} = \widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}/\mathbf{Aut}$, where $\mathbf{Aut}$ denotes the automorphism subgroupoid scheme of $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ which is defined by taking the collection of automorphism groups of all the objects of $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$,

$$\mathbf{Aut} = \coprod_{(\mathcal{E},\omega)} \operatorname{Aut}\mathcal{E}.$$

Notice that the automorphism group of $(\mathcal{E},\omega)$ only depends on $\mathcal{E}$ and so we can safely write $\operatorname{Aut}\mathcal{E}$ for this. The objects of $\boldsymbol{\mathcal{C}}$ are the objects of $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$, whereas the morphism sets are double cosets of the form

$$\boldsymbol{\mathcal{C}}((\mathcal{E}_1,\omega_1),(\mathcal{E}_2,\omega_2)) = \operatorname{Aut}\mathcal{E}_2\backslash\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}((\mathcal{E}_1,\omega_1),(\mathcal{E}_2,\omega_2))/\operatorname{Aut}\mathcal{E}_1.$$

If we denote the twisting automorphism corresponding to $t \in \operatorname{Aut}\mathcal{E} \subseteq \overline{\mathbb{F}}_p^{\times}$ by $\tau_t\colon \mathcal{E} \longrightarrow \mathcal{E}^{t^2}$, where

$$\tau_t(x,y) = (t^2x, t^3y),$$

then an element of $\boldsymbol{\mathcal{C}}((\mathcal{E}_1,\omega_1),(\mathcal{E}_2,\omega_2))$ is an equivalence class of morphisms in $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ of the form

$$\tau_t \circ \varphi \circ \tau_{s^{-1}} \quad (s \in \operatorname{Aut}(\mathcal{E}_1), t \in \operatorname{Aut}(\mathcal{E}_2)),$$

for some fixed morphism $\varphi\colon (\mathcal{E}_1,\omega_1) \longrightarrow (\mathcal{E}_2,\omega_2)$.

Our second quotient category is $\boldsymbol{\mathcal{C}}_0 = \widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}/\boldsymbol{\mu}_{p^2-1}$, where $\boldsymbol{\mu}_{p^2-1}$ denotes the étale subgroupoid scheme of $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ generated by all twistings by elements in the kernel of the (p^2-1)-power map $\mathbb{G}_{\mathrm{m}} \longrightarrow \mathbb{G}_{\mathrm{m}}$, whose points over $\overline{\mathbb{F}}_p$ form the group

$$\mu_{p^2-1}(\overline{\mathbb{F}}_p) = \{t \in \overline{\mathbb{F}}_p^{\times} : t^{p^2-1} = 1\}.$$

Notice that $\mathbf{Aut}$ is a subgroupoid scheme of $\boldsymbol{\mu}_{p^2-1}$. Objects of $\boldsymbol{\mathcal{C}}_0$ are equivalence classes $[\mathcal{E},\omega]$ of objects of $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$, and the morphism set $\boldsymbol{\mathcal{C}}_0([\mathcal{E}_1,\omega_1],[\mathcal{E}_2,\omega_2])$ is a double coset of the form

$$\mu_{p^2-1}\backslash\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}((\mathcal{E}_1,\omega_1),(\mathcal{E}_2,\omega_2))/\mu_{p^2-1}$$

which is the equivalence class consisting of morphisms in $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ of the form

$$\tau_t(x,y) = (t^2x, t^3y),$$

and an element of $\boldsymbol{\mathcal{C}}((\mathcal{E}_1,\omega_1),(\mathcal{E}_2,\omega_2))$ is an equivalence class of morphisms in $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ of the form

$$\tau_t \circ \varphi \circ \tau_{s^{-1}} \quad (s,t \in \mu_{p^2-1}),$$

for some fixed morphism $\varphi\colon (\mathcal{E}_1,\omega_1) \longrightarrow (\mathcal{E}_2,\omega_2)$.

The set of objects in $\boldsymbol{\mathcal{C}}_0$ is represented by the invariant subring

$${}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]^{\mu_{p^2-1}} \subseteq {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}],$$

where the action of μ_{p^2-1} is given by

$$t \cdot xu^n = t^{d+n}x \quad (x \in {}^{\mathrm{ss}}E\ell\ell_{2d},\ t \in \mu_{p^2-1}(\overline{\mathbb{F}}_p)).$$

Furthermore, the set of morphisms of $\boldsymbol{\mathcal{C}}_0$ is represented by the algebra

$${}^{\mathrm{ss}}\Gamma_*^{\mu_{p^2-1}} = {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]^{\mu_{p^2-1}} \underset{\varepsilon}{\otimes} {}^{\mathrm{ss}}\Gamma_* \underset{\varepsilon}{\otimes} {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]^{\mu_{p^2-1}},$$

where the tensor products are formed using the idempotent ring homomorphism

$$\varepsilon\colon {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}] \longrightarrow {}^{\mathrm{ss}}E\ell\ell_*$$

obtained by averaging over the action of μ_{p^2-1} whose image is ${}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]^{\mu_{p^2-1}}$.

Theorem 9.1. *There is a natural isomorphism of groupoids with $\mathbb{G}_{\mathrm{m}}$-action,*

$$\operatorname{Spec}_{\overline{\mathbb{F}}_p} \overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma_*^{\mu_{p^2-1}} \cong \boldsymbol{\mathcal{C}}_0.$$

Moreover, $\overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma_{2n}^{\mu_{p^2-1}}$ can be identified with the set of continuous functions $\boldsymbol{\mathcal{C}}_0 \longrightarrow \overline{\mathbb{F}}_p$ of weight n and ${}^{\mathrm{ss}}\Gamma_{2n}^{\mu_{p^2-1}} \subseteq \overline{\mathbb{F}}_p \otimes {}^{\mathrm{ss}}\Gamma_{2n}^{\mu_{p^2-1}}$ with the subset of Galois invariant functions.

The natural morphism of topological groupoids $\widetilde{\varepsilon}\colon \mathbf{SepIsog}_{\mathrm{ss}}^{\times} \longrightarrow \boldsymbol{\mathcal{C}}_0$ is induced by the natural morphism of Hopf algebroids $\varepsilon\colon ({}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]^{\mu_{p^2-1}}, {}^{\mathrm{ss}}\Gamma_*^{\mu_{p^2-1}}) \longrightarrow ({}^{\mathrm{ss}}E\ell\ell_*, {}^{\mathrm{ss}}\Gamma_*)$ under which u goes to 1. Furthermore, $\widetilde{\varepsilon}$ is an equivalence of topological groupoids.

In the latter part of this result, the topological structure has to be taken into account when discussing equivalences of groupoids, with all the relevant maps required to be continuous. This fact will be used to prove some cohomological results in Section 10. Notice that $\boldsymbol{\mu}_{p^2-1}$ is an étale group scheme and $\widetilde{\varepsilon}$ is an étale morphism.

By Proposition 8.6, $\mathbf{SepIsog}_{\mathrm{ss}}^{\times}$ is connected, hence so are the quotient categories $\boldsymbol{\mathcal{C}}$ and $\boldsymbol{\mathcal{C}}_0$. The following stronger result holds.

Theorem 9.2. *Let $\boldsymbol{\mathcal{E}}_0$ be an object of either of these categories. Then there are continuous maps $\sigma\colon \boldsymbol{\mathcal{C}} \longrightarrow \operatorname{Obj}\boldsymbol{\mathcal{C}}$, $\sigma_0\colon \boldsymbol{\mathcal{C}}_0 \longrightarrow \operatorname{Obj}\boldsymbol{\mathcal{C}}_0$ for which*

$$\operatorname{dom}\sigma(\boldsymbol{\mathcal{E}}) = \operatorname{dom}\sigma_0(\boldsymbol{\mathcal{E}}) = \boldsymbol{\mathcal{E}}_0, \quad \operatorname{codom}\sigma(\boldsymbol{\mathcal{E}}) = \operatorname{codom}\sigma_0(\boldsymbol{\mathcal{E}}) = \boldsymbol{\mathcal{E}}.$$

Hence there are splittings of topological categories

$$\boldsymbol{\mathcal{C}} \cong \operatorname{Obj}\boldsymbol{\mathcal{C}} \rtimes \operatorname{Aut}_{\boldsymbol{\mathcal{C}}}\boldsymbol{\mathcal{E}}_0, \quad \boldsymbol{\mathcal{C}}_0 \cong \operatorname{Obj}\boldsymbol{\mathcal{C}}_0 \rtimes \operatorname{Aut}_{\boldsymbol{\mathcal{C}}_0}\boldsymbol{\mathcal{E}}_0.$$

Proof. We verify this for $\boldsymbol{\mathcal{C}}$, the proof for $\boldsymbol{\mathcal{C}}_0$ being similar. Choose an object $(\mathcal{E}_0, \omega_0)$ of $\boldsymbol{\mathcal{C}}$ and set $\alpha_0 = j(\mathcal{E}_0)$.

First note that for each $\alpha \in \overline{\mathbb{F}}_p$, the subcategory of $\widetilde{\mathbf{SepIsog}}_{\mathrm{ss}}^{\times}$ consisting of objects $(\mathcal{E}, \omega)$ with $j(\mathcal{E}) = \alpha$ is either empty or forms a closed and open set U_α in the natural (Zariski) topology on the space of all such elliptic curves. In each of the non-empty sets U_α, we may pick an element $(\mathcal{E}_\alpha, \omega_\alpha)$. Then for each $(\mathcal{E}, \omega)$ with $j(\mathcal{E}) = \alpha$, there is a non-unique isomorphism $\varphi_{(\mathcal{E},\omega)}\colon (\mathcal{E}_\alpha, \omega_\alpha) \longrightarrow (\mathcal{E}, \omega)$ in **SepIsog**. Given a second such isomorphism φ', the composite $\varphi^{-1} \circ \varphi'$ is in $\operatorname{Aut}\mathcal{E}_\alpha$. Passing to the quotient category $\boldsymbol{\mathcal{C}}$ we see that the image of the subcategory generated by U_α is connected since all such isomorphisms φ have identical images.

Now for every α with U_α non-empty, we may choose a separable isogeny

$$\varphi_\alpha\colon (\mathcal{E}_0, \omega_0) \longrightarrow (\mathcal{E}_\alpha, \omega_\alpha).$$

Again, although this is not unique, on passing to the image set $\overline{U}_\alpha$ in $\boldsymbol{\mathcal{C}}$ we obtain a unique such morphism between the images in $\boldsymbol{\mathcal{C}}$. Forming the composite $\varphi_{(\mathcal{E},\omega)} \circ \varphi_\alpha$ and passing to $\boldsymbol{\mathcal{C}}$ gives a continuous map $\overline{U}_\alpha \longrightarrow \boldsymbol{\mathcal{C}}$ with the desired properties, and then patching together these maps over the finitely many supersingular j-invariants for the prime p establishes the result. $\square$

Corollary 9.3. *There are equivalences of topological categories*

$$\boldsymbol{\mathcal{C}} \simeq \operatorname{Aut}_{\boldsymbol{\mathcal{C}}}\boldsymbol{\mathcal{E}}_0, \quad \boldsymbol{\mathcal{C}}_0 \simeq \operatorname{Aut}_{\boldsymbol{\mathcal{C}}_0}\boldsymbol{\mathcal{E}}_0.$$

Corollary 9.4. *There is an equivalence of Hopf algebroids*

$$({}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]^{\mu_{p^2-1}}, {}^{\mathrm{ss}}\Gamma_*^{\mu_{p^2-1}}) \longrightarrow (K(2)_*, K(2)_*K(2)).$$

10. Some equivalences of Hopf algebroids

Now that we possess the machinery developed in Section 7, we are in a position to give some cohomological results. Our goal is to reprove the following result of [11, theorem 4.1].

Theorem 10.1. *There is an equivalence of Hopf algebroids*

$$(E\ell\ell_*/(p,A), E\ell\ell_*E\ell\ell/(p,A)) \longrightarrow (K(2)_*, K(2)_*K(2)),$$

inducing an isomorphism

$$\operatorname{Ext}^{*,*}_{E\ell\ell_*E\ell\ell}(E\ell\ell_*, E\ell\ell_*/(p,A)) \cong \operatorname{Ext}^{*,*}_{K(2)_*K(2)}(K(2)_*, K(2)_*).$$

First we will make use of a further result of Devinatz [18].

Proposition 10.2. *The natural morphism of Hopf algebroids*

$$({}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}], {}^{\mathrm{ss}}\Gamma_*) \longrightarrow ({}^{\mathrm{ss}}E\ell\ell_*, {}^{\mathrm{ss}}\Gamma^0_*)$$

induces an isomorphism of Ext *groups.*

Proof. See the discussion of [18, Construction 2.7], in particular the remarks between equations (2.8) and (2.9). □

By [30, proposition 1.3d], we have

$$\begin{aligned}\operatorname{Ext}^{*,*}_{E\ell\ell_*E\ell\ell}(E\ell\ell_*, E\ell\ell_*/(p,A)) &\cong \operatorname{Ext}^{*,*}_{{}^{\mathrm{ss}}\Gamma^0_*}({}^{\mathrm{ss}}E\ell\ell_*, {}^{\mathrm{ss}}E\ell\ell_*)\\ &\cong \operatorname{Ext}^{*,*}_{{}^{\mathrm{ss}}\Gamma_*}({}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}], {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]).\end{aligned}$$

By Theorem 9.1, there is an isomorphism

$$\begin{aligned}&\operatorname{Ext}^{*,*}_{{}^{\mathrm{ss}}\Gamma_*}({}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}], {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}])\\ &\qquad\cong \operatorname{Ext}^{*,*}_{{}^{\mathrm{ss}}\Gamma_*^{\mu_{p^2-1}}}({}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]^{\mu_{p^2-1}}, {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]^{\mu_{p^2-1}}).\end{aligned}$$

Finally, by Corollary 9.4 there is an isomorphism

$$\begin{aligned}&\operatorname{Ext}^{*,*}_{{}^{\mathrm{ss}}\Gamma_*^{\mu_{p^2-1}}}({}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]^{\mu_{p^2-1}}, {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]^{\mu_{p^2-1}})\\ &\qquad\cong \operatorname{Ext}^{*,*}_{K(2)_*K(2)}(K(2)_*, K(2)_*).\end{aligned}$$

11. Isogenies and stable operations in supersingular elliptic cohomology

In this section we explain how the category $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ naturally provides a model for a large part of the stable operation algebra of supersingular elliptic cohomology ${}^{\mathrm{ss}}E\ell\ell^*(\ )$. In fact, it turns out that the subalgebra ${}^{\mathrm{ss}}E\ell\ell^*E\ell\ell = {}^{\mathrm{ss}}E\ell\ell^*(E\ell\ell)$ can be described as a subalgebra of the 'twisted topologized category algebra' of $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$ with coefficients in ${}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]$. Such a clear description is not available for $E\ell\ell^*E\ell\ell = E\ell\ell^*(E\ell\ell)$, although an analogous result for the stable operation algebra $K(1)^*(E(1))$ is well known with the later being a twisted topological group algebra. More generally, Morava and his interpreters have given analogous descriptions of $K(n)^*(E(n))$ for $n \geqslant 1$.

By [4], ${}^{\mathrm{ss}}E\ell\ell_*$ and ${}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]$ are products of 'graded fields', hence

$$\begin{aligned}{}^{\mathrm{ss}}E\ell\ell^*E\ell\ell &= \operatorname{Hom}_{{}^{\mathrm{ss}}E\ell\ell_*}({}^{\mathrm{ss}}E\ell\ell_*(E\ell\ell), {}^{\mathrm{ss}}E\ell\ell_*),\\ {}^{\mathrm{ss}}E\ell\ell[u,u^{-1}]^*E\ell\ell &= \operatorname{Hom}_{{}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}]}({}^{\mathrm{ss}}E\ell\ell[u,u^{-1}]_*(E\ell\ell), {}^{\mathrm{ss}}E\ell\ell_*[u,u^{-1}].\end{aligned}$$

The set of all morphisms originating at a particular object $\underline{\mathcal{E}_0} = (\mathcal{E}_0, \omega_0)$ of $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$, with defined over $\mathbb{F}_p$ (such curves always exist by Theorem A.1), is

$$\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}(\underline{\mathcal{E}_0}, *) = \coprod_{\substack{\underline{\mathcal{E}} \text{ isogenous} \\ \text{to } \underline{\mathcal{E}_0}}} \widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}(\underline{\mathcal{E}_0}, \underline{\mathcal{E}}),$$

is noncanonically a product of the form

$$\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}(\underline{\mathcal{E}_0}, *) = \coprod_{(\mathcal{E}_0/N, \omega_0)} \mathrm{InvtHom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p(\mathcal{E}_0/N), \mathcal{T}_p\mathcal{E}_0) \times \overline{\mathbb{F}}_p^{\times},$$

where N ranges over the finite subgroups of $\mathcal{E}_0$ of order prime to p.

Using similar methods to those of [5, 8] we can construct stable operations T_n $(p \nmid n)$ in the cohomology theory ${}^{\mathrm{ss}}E\ell\ell_*[u, u^{-1}]^*(\ )$ and these actually restrict to operations in ${}^{\mathrm{ss}}E\ell\ell^*_*(\ )$. These operations (together with Adams-like operations originating on the factor of $\overline{\mathbb{F}}_p$) generate a Hecke-like algebra.

There is also a further set of operations coming from elements of the component

$$\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}(\underline{\mathcal{E}_0}, \underline{\mathcal{E}_0}) = \mathrm{InvtHom}_{\mathbb{D}_{\overline{\mathbb{F}}_p}}(\mathcal{T}_p(\mathcal{E}_0), \mathcal{T}_p\mathcal{E}_0) \times \overline{\mathbb{F}}_p^{\times}.$$

These operations correspond to the Hecke-like algebra of [8] associated to the Morava stabilizer group $\mathbb{S}_2$.

Combining these two families of operations gives rise to a composite Hecke-like algebra which in turn generates subalgebras of the operation algebras in the cohomology theories ${}^{\mathrm{ss}}E\ell\ell_*[u, u^{-1}]^*(\ )$ and ${}^{\mathrm{ss}}E\ell\ell^*_*(\ )$.

12. Relationship with work of Robert

In [33], Robert discussed the action of Hecke operators T_n $(p \nmid n)$ on the ring of holomorphic modular forms modulo the supersingular ideal generated by p, A, in effect studying the action of the étale part of the category $\widetilde{\mathbf{SepIsog}}^{\times}_{\mathrm{ss}}$. In this section we discuss connections between this work and ours. Serre [35] gave an adelic description of Hecke operators associated to supersingular elliptic curves which appears to have connections with our work.

We begin with some comments on Robert's work which provides a classical Hecke operator perspective on ours. We denote by $\mathrm{B}\colon {}^{\mathrm{ss}}E\ell\ell_* \longrightarrow {}^{\mathrm{ss}}E\ell\ell_*$ the operator $\mathrm{B}(F) = BF$, which raises weight by $p+1$ and degree by $2(p+1)$. The following operator commutativity formula holds for all primes $\ell \neq p$:

$$\mathrm{B}\mathrm{T}_\ell = \ell \mathrm{T}_\ell \mathrm{B}. \tag{12.1}$$

This is actually a more general result than Robert proves since he only works with holomorphic modular forms, but our result of [9], discussed earlier in Theorem 3.2, gives in the ring ${}^{\mathrm{ss}}E\ell\ell_*$

$$B^{p-1} = -\left(\frac{-1}{p}\right)\Delta^{(p^2-1)/12},$$

and this allows us to localize with respect to powers of Δ or equivalently of B.

Recall the Hecke algebra

$$\mathbf{H}_p = \mathbb{F}_p[\mathrm{T}_\ell, \psi^\ell : \text{primes } \ell \neq p]/(\text{relations}),$$

where the relations are the usual ones satisfied by Hecke operations, as described in Theorem 7 of [5]. We follow Robert in introducing certain twistings of a module M. For each natural number a let $M[a]$ denote underlying $\mathbb{F}_p$-module M with the twisted Hecke action

$$\mathrm{T}_\ell \cdot m = \mathrm{T}_\ell^{[a]} m = \ell^a \mathrm{T}_\ell m.$$

When $F \in {}^{\mathrm{ss}}E\ell\ell_*$, this agrees with Robert's action

$$\mathrm{T}_\ell^{[a]} F = \ell^a \mathrm{T}_\ell F,$$

at least when restricted to the holomorphic part, and then $M[a] \cong M[a+p-1]$ as $\mathbf{H}_p$-modules since $\ell^{p-1} \equiv 1 \bmod (p)$. We view multiplication by B as giving rise to homomorphisms of graded $\mathbf{H}_p$-modules $\mathrm{B}\colon {}^{\mathrm{ss}}E\ell\ell_*[a] \longrightarrow {}^{\mathrm{ss}}E\ell\ell_*[a-1]$ for $a \in \mathbb{Z}$, uniformly raising degrees by $2(p+1)$.

More generally, if M_* is a right comodule over the Hopf algebroid $({}^{\mathrm{ss}}E\ell\ell_*, {}^{\mathrm{ss}}\Gamma^0_*)$ with coproduct $\gamma\colon M \longrightarrow M \underset{{}^{\mathrm{ss}}E\ell\ell_*}{\otimes} {}^{\mathrm{ss}}\Gamma^0_*$, then associated to each $a \in \mathbb{Z}$ there is a twisted comodule $M_*[a]$ with coproduct

$$\gamma^{[a]} m = \sum_i m_i \otimes t_i \,\mathrm{ind}^a,$$

where ind is defined in Equation 5.1 (see also Proposition 5.2) and $\gamma m = \sum_i m_i \otimes t_i$.

Recall that for any left ${}^{\mathrm{ss}}E\ell\ell_*$-linear map $\theta\colon {}^{\mathrm{ss}}\Gamma^0_* \longrightarrow {}^{\mathrm{ss}}E\ell\ell_*$ there is an operation $\overline{\theta}$ on M_* given by

$$\overline{\theta} m = \sum_i m_i \otimes \theta(t_i).$$

By [5, 8], this construction gives rise to an induced $\mathbf{H}_p$-module structures on M_* and $M_*[a]$ agreeing with that generalizing Robert's discussed above. In fact, these extend to module structures over the associated *twisted Hecke algebra* containing ${}^{\mathrm{ss}}E\ell\ell_*$ and $\mathbf{H}_p$ as discussed in [8]. Also there are homomorphisms $\mathrm{B}\colon M_*[a] \longrightarrow M_*[a-1]$ of modules over the twisted Hecke algebra and induced from multiplication by B. The following is our analogue of [33, lemme 6].

Theorem 12.1. *For $a \in \mathbb{Z}$, $\mathrm{B}\colon M_*[a] \longrightarrow M_*[a-1]$ defines an isomorphism of $({}^{\mathrm{ss}}E\ell\ell_*, {}^{\mathrm{ss}}\Gamma^0_*)$-comodules.*

Proof. We make use of the description of $E\ell\ell_* E\ell\ell_{(p)}$ from [6] and view modular forms as functions on the space of oriented lattices in $\mathbb{C}$. As will see, the argument used by Robert to determine $\mathrm{T}_\ell B$ for a prime $\ell \neq p$ is based on a congruence in $E\ell\ell_* E\ell\ell_{(p)}$.

By [33, equation 19, théorème B/lemme 7], we have the following. If for some $r = 0, 1, \dots \ell-1$,

$$L = \langle \tau, 1 \rangle \subseteq \langle \tau', 1 \rangle, \quad \tau' = \frac{\tau + r}{\ell}, \quad q' = e^{2\pi i \tau'},$$

then taking q-expansions over $\mathbb{Z}_{(p)}$ gives

$$B(q') - B(q) \equiv -12 \sum_{1 \leqslant s \leqslant \ell-1} \sum_{1 \leqslant k} \left(\frac{q^k (q')^s}{(1 - q^k (q')^s)^2} + \frac{q^k (q')^{-s}}{(1 - q^k (q')^{-s})^2} \right) \bmod (p).$$

On the other hand, if

$$L = \langle \tau, 1 \rangle \subseteq \left\langle \tau, \frac{1}{\ell} \right\rangle, \quad \tau' = \ell\tau, \quad q' = e^{2\pi i \tau'},$$

then by taking q-expansions we obtain

$$\ell^{p+1} B(q') - B(q) \equiv$$
$$\sum_{1 \leqslant s \leqslant \ell-1} \left((\ell^2 - 1) B(q) - 12\ell^2 \sum_{1 \leqslant k} \left(\frac{q^k (q')^s}{(1 - q^k (q')^s)^2} + \frac{q^k (q')^{-s}}{(1 - q^k (q')^{-s})^2} \right) \right) \bmod (p).$$

In the terminology of [6], the coefficient of each monomial $q^u (q')^v$ is a stably numerical polynomial in ℓ. Indeed, using the integrality criterion of [6, theorem 6.3] for generalized modular

forms to lie in $E\ell\ell_*E\ell\ell_{(p)}$, together with the fact that every lattice inclusion of index not divisible by p factors into a sequence of lattice inclusions of prime index, we can obtain similar formulæ for all lattice inclusions of (not necessarily prime) index not divisible by p.

The precise interpretation of what is going on here is that there are functions $F_0, F_1 \in E\ell\ell_*E\ell\ell_{(p)}$ on inclusions of lattices such that for any inclusion of lattices $L \subseteq L'$ of degree $[L'; L]$ not divisible by p,

$$B(L') - [L'; L]B(L) = pF_0(L \subseteq L') + A(L)F_1(L \subseteq L'). \tag{12.2}$$

It follows from this that in the ring $E\ell\ell_*E\ell\ell_{(p)}$,

$$\eta_R(B) - \eta_L(B)\,\mathrm{ind} \equiv 0 \bmod (p, A_1), \tag{12.3}$$

Notice that under the reduction map $E\ell\ell_*E\ell\ell_{(p)} \longrightarrow {}^{\mathrm{ss}}\Gamma^0_*$, the index function

$$(L \subseteq L') \longmapsto [L'; L]$$

is sent to ind. This can be seen as follows. For any supersingular elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_{p^2}$ there is an imaginary quadratic number field K in which p is unramified and so there is a lift α of $j(\mathcal{E})$ contained in the ring of integers $\mathcal{O}_K$. Then there is an elliptic curve $\widetilde{\mathcal{E}}$ defined over $\mathcal{O}_K$ with $j(\widetilde{\mathcal{E}}) = \alpha$ and reduction modulo p induces an isomorphism $\widetilde{\mathcal{E}}[n] \longrightarrow \mathcal{E}[n]$ for $p \nmid n$. Since a strict (hence separable) isogeny $\varphi\colon \mathcal{E} \longrightarrow \mathcal{E}'$ of degree n, and defined over an extension of $\mathbb{F}_{p^2}$ is determined by $\ker\varphi \subseteq \mathcal{E}[n]$, it can be lifted to a strict isogeny $\widetilde{\varphi}\colon \widetilde{\mathcal{E}} \longrightarrow \widetilde{\mathcal{E}'}$ of degree n and defined over some extension of $\mathcal{O}_K$, where $\ker\widetilde{\varphi}$ is the preimage of $\ker\varphi$ under reduction. Then $\mathrm{ind}\,\varphi \equiv n \bmod (p)$. Hence if we express $\widetilde{\mathcal{E}}$ in the form $\mathbb{C}/L$, $\widetilde{\mathcal{E}'}$ can be realized as $\mathbb{C}/L'$ where $L \subseteq L'$ has index n.

Because $\mathrm{ind}^{p-1} = c_1$ (the constant function taking value 1), we have

$$\eta_R(B^{p-1}) - \eta_L(B^{p-1}) \equiv 0 \bmod (p, A_1), \tag{12.4}$$

which implies that $B^{p-1} \in {}^{\mathrm{ss}}E\ell\ell_*$ is coaction primitive.

By Equation (12.2), we have

$$\begin{aligned}
\gamma\mathrm{B}(m) = \gamma(mB) &= \sum_i m_i \otimes t_i\eta_R B \\
&= \sum_i m_i \otimes Bt_i\,\mathrm{ind} \\
&= \sum_i m_iB \otimes t_i\,\mathrm{ind} \\
&= \sum_i \mathrm{B}(m_i) \otimes t_i\,\mathrm{ind} \\
&= \mathrm{B}\gamma^{[1]}m,
\end{aligned}$$

where we have viewed M_* as a right ${}^{\mathrm{ss}}E\ell\ell_*$-module and used ${}^{\mathrm{ss}}E\ell\ell_*$-bimodule tensor products.

The determination of $\mathrm{T}_\ell B$ now follows from our definition of the Hecke operators of [6, equation 6.5], as does the generalization of Robert's formula

$$\mathrm{T}_\ell(BF) \equiv \ell B\mathrm{T}_\ell(F),$$

which holds for $F \in {}^{\mathrm{ss}}E\ell\ell_*$, and primes $\ell \neq p$. □

Our results are more general than those of Robert since they involve generalized isogenies rather than just isogenies to define ${}^{\mathrm{ss}}E\ell\ell_*$-linear maps ${}^{\mathrm{ss}}\Gamma^0_* \longrightarrow \overline{\mathbb{F}}_p$ and hence operations $\overline{\varphi}$

on ${}^{\mathrm{ss}}\Gamma^0_*$-comodules. Explicit operations of this type were defined in [8] using Hecke operators derived from the space of double cosets

$$\langle \mu_{p^2-1}, p\rangle \backslash \widetilde{\mathbb{S}}_2 / \langle \mu_{p^2-1}, p\rangle$$

and its associated Hecke algebra; in fact this space is homeomorphic to $\underset{\sim}{\mathbb{S}^0_2 \rtimes \mathbb{Z}/2}$ as a space. For each supersingular elliptic curve $(\mathcal{E}, \omega)$ we can identify $\mathbb{W}(\mathbb{F}_{p^2})\langle \mathrm{S}\rangle$ with $\widetilde{\mathbf{Isog}}((\mathcal{E},\omega),(\mathcal{E},\omega))$ and as in [8] obtain for each $\alpha \in \mathbb{S}_2 \rtimes \mathbb{Z}/2$ an ${}^{\mathrm{ss}}E\ell\ell_*$-linear map $\alpha_* \colon {}^{\mathrm{ss}}\Gamma^0_* \longrightarrow {}^{\mathrm{ss}}E\ell\ell_*$ and hence an operation $\overline{\alpha}$ on ${}^{\mathrm{ss}}\Gamma^0_*$-comodules. This can be further generalized by associating to each positive integer d and each separable isogeny $(\mathcal{E},\omega) \xrightarrow{\varphi} (\mathcal{E}',\omega')$ of degree d, the corresponding element $\alpha^{\varphi} \in \widetilde{\mathbf{Isog}}((\mathcal{E},\omega),(\mathcal{E}',\omega'))$ and then symmetrizing over all of these to form a ${}^{\mathrm{ss}}E\ell\ell_*$-linear map

$$\alpha^d_* \colon {}^{\mathrm{ss}}\Gamma^0_* \longrightarrow {}^{\mathrm{ss}}E\ell\ell_*; \quad (\alpha^d_* F)(\mathcal{E},\omega) = \frac{1}{d}\sum_{\varphi} \alpha^{\varphi}_*.$$

Robert analyzes the holomorphic part of ${}^{\mathrm{ss}}E\ell\ell_{2n}$ as a $\mathbf{H}_p$-module, in particular he determines when the *Eisenstein modules* Ei_k embed, where Ei_k is the 1-dimensional $\mathbb{F}_p$-module on the generator e_k for which

$$\mathrm{T}_{\ell} e_k = (1+\ell^{k-1})e_k.$$

Thus Ei_k is an eigenspace for each Hecke operator T_{ℓ}, and there is an isomorphism of $\mathbf{H}_p$-modules

$$\mathrm{Ei}_{2k} \cong \mathbb{F}_p\{\widetilde{E}_{2k}\} \subseteq {}^{\mathrm{ss}}E\ell\ell_{4k}; \quad e_{2k} \longmapsto \widetilde{E}_{2k},$$

where $\widetilde{E}_{2k}$ is the reduction of one of the following elements of $(E\ell\ell_{2k})_{(p)}$:

$$\begin{cases} E_{2k} & \text{if } (p-1) \mid 2k, \\ (B_{2k}/4k)E_{2k} & \text{if } (p-1) \nmid 2k. \end{cases}$$

In particular, Ei_0 is the 'trivial' module for which

$$\mathrm{T}_{\ell} e_0 = (1+\ell^{-1})e_0.$$

Robert gives conditions on when there is an occurrence of Ei_k in ${}^{\mathrm{ss}}E\ell\ell_{2n}$, at least in the holomorphic part. Since localization with respect to powers of Δ is equivalent to that with respect to powers of B by the main result of [9] we can equally well apply his results to ${}^{\mathrm{ss}}E\ell\ell_{2n}$, obtaining the following version of [33, théorème 3].

Theorem 12.2. *For a prime $p \geqslant 5$ and an even integer k, there is an embedding of $\mathbf{H}_p$-modules $\mathrm{Ei}_k \longrightarrow {}^{\mathrm{ss}}E\ell\ell_{2n}$ if and only if one of the following congruences holds:*

$$n \equiv k \bmod (p^2-1), \quad n \equiv pk \bmod (p^2-1).$$

Notice that in particular, the trivial module Ei_0 occurs precisely in degrees $2n$ for which $(p^2-1) \mid 2n$. The Ext groups of ${}^{\mathrm{ss}}E\ell\ell_*$ over ${}^{\mathrm{ss}}\Gamma^0_*$ were investigated in [11, 10], and the results show that Robert's conditions are weaker than needed to calculate $\underset{\sim}{\mathrm{Ext}^0}$. Of course, his work ignores the effect of operations coming from the 'connected' part of $\mathbf{SepIsog}^{\times}_{\mathrm{ss}}$.

Appendix A. Supersingular curves defined over $\mathbb{F}_p$

For every prime $p > 3$ with $p \not\equiv 1 \bmod (12)$ there are supersingular elliptic curves defined over $\mathbb{F}_p$ since the Hasse invariant then has Q or R as a factor. The following stronger result which seems to be due to Deuring is also true and a sketch proof can be found in [9]; Cox [16] also contains an accessible account of related material.

Let $\mathcal{E}$ be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ whose j-invariant is $j(\mathcal{E}) \equiv 0 \bmod (p)$ or $1728 \bmod (p)$. Recall that the endomorphism ring $\operatorname{End}\mathcal{E}$ contains an imaginary quadratic number ring of the form

$$\begin{cases} \mathbb{Z}[\omega] & \text{if } j(\mathcal{E}) \equiv 0 \bmod (p), \\ \mathbb{Z}[i] & \text{if } j(\mathcal{E}) \equiv 1728 \bmod (p). \end{cases}$$

By Theorem 1.4, such elliptic curves are isomorphic to Weierstraß curves defined over $\mathbb{F}_p$.

Let $K = \mathbb{Q}(\sqrt{-p})$ and $\mathcal{O}_K$ be its ring of integers which is its unique maximal order.

Theorem A.1. *For any prime $p > 11$, there are supersingular elliptic curves $\mathcal{E}$ defined over $\mathbb{F}_p$ with $j(\mathcal{E}) \not\equiv 0, 1728 \bmod (p)$ and $\mathcal{O}_K \subseteq \operatorname{End}\mathcal{E}$.*

References

[1] J. F. Adams, Stable Homotopy and Generalised Homology, University of Chicago Press (1974).

[2] A. Baker, p-adic continuous functions on rings of integers, J. Lond. Math. Soc. **33** (1986), 414–20.

[3] ———, Elliptic cohomology, p-adic modular forms and Atkin's operator U_p, Contemp. Math. **96** (1989), 33–38.

[4] ———, On the homotopy type of the spectrum representing elliptic cohomology, Proc. Amer. Math. Soc. **107** (1989), 537–48.

[5] ———, Hecke operators as operations in elliptic cohomology, J. Pure Appl. Algebra **63** (1990), 1–11.

[6] ———, Operations and cooperations in elliptic cohomology, Part I: Generalized modular forms and the cooperation algebra, New York J. Math. **1** (1995), 39–74.

[7] ———, A version of the Landweber filtration theorem for v_n-periodic Hopf algebroids, Osaka J. Math. **32** (1995), 689–99.

[8] ———, Hecke algebras acting on elliptic cohomology, Contemp. Math. **220** (1998), 17–26.

[9] ———, A supersingular congruence for modular forms, Acta Arithmetica **85** (1998), 91–100.

[10] ———, Hecke operations and the Adams E_2-term based on elliptic cohomology, Can. Math. Bull. **42** (1999), 129–138.

[11] ———, On the Adams E_2-term for elliptic cohomology, Contemp. Math. **271** (2001), 1–15.

[12] ———, Profinite groupoids and their cohomology, Glasgow University Mathematics Department preprint 99/33.

[13] H-J. Baues & G. Wirsching, Cohomology of small categories, J. Pure Appl. Algebra **38** (1985), 187–211.

[14] M. Behrens & T. Lawson, Isogenies of elliptic curves and the Morava stabilizer group, to appear in J. Pure Appl. Alg., `arXiv:math/0508079`.

[15] M. Behrens & T. Lawson, Topological automorphic forms, `arXiv:math/0702719`.

[16] D. A. Cox, Primes of the form x^2+ny^2, Fermat, class field theory and complex multiplication, Wiley (1989).

[17] M. Demazure, Lectures on p-divisible groups, Lecture Notes in Mathematics **302** (1972).

[18] E. Devinatz, Morava's change of rings theorem, Contemp. Math. **181** (1995), 83–118.

[19] J-M. Fontaine, Groupes p-divisibles sur les corps locaux, Astérisque **47–48** (1977).

[20] M. Hazewinkel, Formal Groups and Applications, Academic Press (1978).

[21] P. J. Higgins, Notes on Categories and Groupoids, Van Nostrand Reinhold (1971).

[22] D. Husemoller, Elliptic Curves, Springer-Verlag (1987).

[23] N. M. Katz, Divisibilities, congruences, and Cartier duality, Astérisque **28** (1981), 667–78.

[24] N. M. Katz, Serre-Tate local moduli, Lecture Notes in Mathematics **868** (1981), 138–202.

[25] N. M. Katz, p-adic properties of modular schemes and modular forms, Lecture Notes in Mathematics **350** (1973), 69–190.

[26] N. M. Katz & B. Mazur, Arithmetic Moduli of Elliptic Curves, Annals of Mathematics Studies **108** (1985).

[27] P. S. Landweber, Homological properties of comodules over MU_*MU and BP_*BP, Amer. J. Math. **98** (1976), 591–610.

[28] ———, Supersingular elliptic curves and congruences for Legendre polynomials, Lecture Notes in Mathematics **1326** (1988), 69–93.

[29] P. S. Landweber, D. C. Ravenel & R. E. Stong, Periodic cohomology theories defined by elliptic curves, Contemp. Math. **181** (1995) 317–337.

[30] H. R. Miller & D. C. Ravenel, Morava stabilizer algebras and localization of Novikov's E_2-term, Duke Math. J. **44** (1977), 433–47.

[31] J. S. Milne, Extensions of abelian varieties defined over a finite field, Invent. Math. **5** (1968), 63–84.

[32] D. C. Ravenel, Complex Cobordism and the Stable Homotopy Groups of Spheres, Academic Press (1986).
[33] G. Robert, Congruences entre séries d'Eisenstein, dans le cas supersingular, Invent. Math. **61** (1980), 103–158.
[34] H-G. Rück, A note on elliptic curves over finite fields, Math. Comp. **49** (1987), 301–4.
[35] J-P. Serre, Unpublished lecture notes.
[36] S. Shatz, Profinite Groups, Arithmetic and Geometry, Annals of Mathematics Studies **67** (1972).
[37] J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag (1986).
[38] N. Strickland, Formal schemes and formal groups, Contemp. Math. **239** (1999), 263–352.
[39] J. Tate, The arithmetic of elliptic curves, Invent. Math. **23** (1974), 179–206.
[40] ———, Endomorphisms of abelian varieties over finite fields, Invent. Math. **2** (1966), 134–144.
[41] J. Vélu, Isogenies entre courbes elliptiques, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), 238–241.
[42] W. C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.
[43] W. C. Waterhouse & J. S. Milne, Abelian varieties over finite fields, Proc. Sympos. Pure Math. **XX** (1971), 53–64.
[44] C. A. Weibel, An Introduction to Homological Algebra, Cambridge University Press (1994).
[45] N. Yagita, The exact functor theorem for BP_*/I_n, Proc. Jap. Acad. **52** (1976), 1–3.

Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland.
E-mail address: `a.baker@maths.gla.ac.uk`
URL: `http://www.maths.gla.ac.uk/~ajb`